

VISIT...

LANZAROTE  
*Caliente*.COM

АКАДЕМИЯ НАУК СОЮЗА ССР

~ КЛАССИКИ НАУКИ ~







КАРЛ ФРИДРИХ ГАУСС  
ТРУДЫ  
ПО ТЕОРИИ ЧИСЕЛ

ОБЩАЯ РЕДАКЦИЯ  
АКАДЕМИКА И. М. ВИНОГРАДОВА  
КОММЕНТАРИИ  
ЧЛЕНА-КОРР. АН СССР Б. Н. ДЕЛОНЕ  
ПЕРЕВОД  
КАНД. ФИЗ.-МАТЕМ. НАУК  
В. Б. ДЕМЬЯНОВА

$$a \equiv b \pmod{m}$$

ИЗДАТЕЛЬСТВО АКАДЕМИИ НАУК СССР  
МОСКВА • 1959

СЕРИЯ «КЛАССИКИ НАУКИ»

основана академиком *С. И. Вавиловым*

Редакционная коллегия: академик *И. Г. Петровский*  
(председатель), академик *Н. Н. Андреев*, академик *Б. А. Казанский*,  
академик *Д. И. Щербаков*, академик *П. Ф. Юдин*, член-корреспондент  
АН СССР *Б. И. Делоне*, член-корреспондент АН СССР *Х. С. Коштойнц*,  
член-корреспондент АН СССР *А. М. Самарин*, профессор *Д. М. Лебедев*,  
профессор *Н. А. Фигуровский*, кандидат философских наук  
*И. В. Кузнецов* (зам. председателя)





# АРИФМЕТИЧЕСКИЕ ИССЛЕДОВАНИЯ





## ПРЕДИСЛОВИЕ АВТОРА

Содержащиеся в этом сочинении исследования относятся к той части математики, которая имеет дело с целыми числами, в то время как дробные числа остаются вне рассмотрения в большинстве случаев, а мнимые — всегда. Так называемый неопределенный или диофантов анализ, представляющий собой учение о том, как из бесконечного числа решений, удовлетворяющих неопределенному уравнению, выбирать те, которые являются целочисленными или хотя бы рациональными (а в большинстве случаев еще и положительными), не исчерпывает этой дисциплины, а представляет собой лишь очень специальную ее часть, которая относится ко всей дисциплине приблизительно так же, как учение о преобразовании и решении уравнений (алгебра) относится к анализу в целом. Именно, как все исследования, которые касаются общих свойств числовых величин и связей между ними, принадлежат к области анализа, так целые числа (а также и дробные, поскольку они определяются через целые) составляют предмет изучения арифметики. Но так как то, что обычно принято называть арифметикой, почти не выходит за пределы искусства считать и вычислять (т. е. представлять числа в определенном виде, например, в десятичной системе, и производить над ними арифметические операции) с добавлением еще некоторых вопросов, которые или вовсе не относятся к арифметике, как, например, учение о логарифмах, или имеют силу не только для целых чисел, но и для любых числовых величин, то представляется целесообразным различать две части арифметики и только что упомянутое причислять к элементарной арифметике, а все общие исследования о внутренних связях между целыми числами относить к высшей арифметике, о которой одной здесь и будет идти речь.



К высшей арифметике относится то, что Э в к л и д с присущими древним изяществом и строгостью изложил в *«Началах»*, в книге VII и следующих; однако это представляет собой лишь первые шаги этой науки. Знаменитое сочинение Д и о ф а н т а, целиком посвященное проблемам неопределенного анализа, содержит много исследований, которые вследствие их трудности и красоты методов заставляют быть высокого мнения об уме и проницательности их автора, особенно, если учесть незначительность вспомогательных средств, находившихся в его распоряжении. Так как, однако, эти задачи больше требуют находчивости и сообразительности, чем глубоких методов, и, кроме того, являются слишком специальными и редко приводят к более общим выводам, то эта книга рассматривается как эпоха в развитии математики скорее потому, что она содержит в себе первые следы искусства, характерного для алгебры, а не потому, что она обогатила новыми открытиями высшую арифметику. Главным образом более поздним исследователям, правда, немногочисленным, но завоевавшим непреходящую славу,— таким, как Ф е р м а, Э й л е р, Л а г р а н ж, Л е ж а н д р, мы обязаны тем, что они нашли доступ к сокровищнице этой божественной науки и показали, какими богатствами она наполнена. Я, однако, не буду здесь перечислять, какие открытия принадлежат каждому из этих математиков в отдельности, так как это можно узнать из предисловия к дополнениям, которыми Л а г р а н ж снабдил *«Алгебру»* Э й л е р а, и из недавно вышедшего сочинения Л е ж а н д р а, о котором скоро будет упоминаться; кроме того, об этом говорится в соответствующих местах настоящих *«Арифметических исследований»*.

Целью этого труда, издать который я обещал еще пять лет назад, было довести до общего сведения те исследования по высшей арифметике, которыми я занимался частью ранее, частью позже указанного срока. Однако, чтобы никто не удивлялся, что я здесь повторяю предмет почти с самого начала и заново произвожу многие исследования, которыми уже занимались другие, я считаю необходимым указать на то, что когда я в начале 1795 г. впервые принялся за исследования такого рода, я ничего не знал о том, что было сделано за последнее время в этой области, и все средства, при помощи ко-

торых я получал свои результаты, я изобретал сам. Именно, занимаясь в то время другой работой, я случайно натолкнулся на одну изумительную арифметическую истину (если не ошибаюсь, она изложена в виде теоремы в п. 108), и так как она не только показалась мне прекрасной сама по себе, но и навела на мысль, что она связана и с другими выдающимися фактами, я со всей энергией взялся за то, чтобы выяснить принципы, на которых она основывается, и получить строгое ее доказательство. После того как это желание, наконец, осуществилось, прелесть этих исследований настолько увлекла меня, что я уже не мог их оставить; так и получилось, что в то время как одни все время пролагали дорогу другим в том, что изложено в первых четырех разделах этого труда, я сам имел о подобных работах других математиков лишь приблизительное представление. Когда же мне, наконец, представилась возможность ознакомиться с работами этих выдающихся умов, то я понял, что большая часть моих рассуждений была посвящена уже давно известным вещам, но с тем большей охотой решился следовать по стопам этих ученых, которые двигали арифметику вперед; так возникли различные исследования, часть которых составляют разделы V, VI, VII. Когда я, спустя некоторое время, принял решение опубликовать результаты моих усилий, то я, идя навстречу желаниям многих, тем охотнее решил не выбрасывать ничего также и из указанных более ранних исследований, что, во-первых, в то время еще не было книги, по которой можно было бы ознакомиться с рассеянными по академическим изданиям работами других математиков по этому вопросу; затем, потому, что многие из этих исследований были совершенно новыми и проводились новыми методами, и, наконец, потому, что все они так тесно переплетались как между собой, так и с более поздними исследованиями, что новое неудобно было бы изложить достаточно ясно без того, чтобы сначала не напомнить некоторые другие вещи.

Тем временем появилось сочинение уже и до того имевшего большие заслуги в высшей арифметике Л е ж а н д р а («*Essai d'une theorie des nombres*», *Paris, a. VI*), в котором он не только тщательно обработал и привел в порядок все, что было сделано в этой науке до сих пор, но и привнес очень много своего собственного. Так как эта

книга попала ко мне в руки слишком поздно, когда бóльшая часть моего сочинения была уже готова, я ее нигде не упоминал в тех случаях, когда аналогия рассматриваемых вопросов могла бы дать к этому повод; лишь в отношении нескольких ее мест я счел необходимым сделать некоторые замечания в дополнениях, которые, как я надеюсь, любознательный читатель не оставит без внимания.

Во время печатания этого сочинения, которое несколько раз прерывалось и из-за многочисленных задержек растянулось на четыре года, я не только продолжил далее те исследования, которые начал еще ранее, но опубликование которых решил отложить до другого случая, чтобы не делать книгу слишком объемистой, но и принялся за многие новые исследования. Кроме того, несколько исследований, которые я по той же причине только вскользь упоминал, так как более подробное рассмотрение представлялось менее необходимым (например, те, о которых говорится в пп. 37, 82 и следующих, и в других местах), в дальнейшем были продолжены и дали повод к более общим исследованиям, которые представляются достойными опубликования (ср. также сказанное в дополнениях относительно п. 306). Наконец, так как книга вследствие значительного размера раздела V оказалась гораздо объемистее, чем я ожидал, — многое, что первоначально для нее предназначалось, и в частности весь восьмой раздел (который в этом сочинении уже упоминается в нескольких местах, и который содержит общее изложение теории алгебраических сравнений любой степени), пришлось выбросить. Все эти вещи, которые легко могут заполнить том, равносильный настоящему, я опубликую, как только для этого представится случай.

То, что во многих трудных исследованиях я пользовался синтетическими доказательствами и опускал анализ, при помощи которого они были найдены, объясняется главным образом требованиями краткости, которым я, насколько это возможно, должен был стремиться удовлетворить.

Теория деления круга или теория правильных многоугольников, которая рассматривается в разделе VII, сама по себе не принадлежит арифметике; однако ее принципы следует черпать только в

высшей арифметике; это будет для математиков, быть может, столь же неожиданным, сколь, надо надеяться, приятными бывают для них обычно истины, черпаемые из этого источника.

На это я хотел обратить внимание читателя. О самом предмете судить не мне. Я ничего не желаю столь горячо, как того, чтобы эти исследования понравились тем, кто принимает близко к сердцу успехи науки, как те, которые восполняют имевшиеся до сих пор пробелы, так и те, что открывают путь к новому.

---



# РАЗДЕЛ I

## О СРАВНИМОСТИ ЧИСЕЛ ВООБЩЕ

### Сравнимые числа, модули, вычеты и невычеты

#### 1

Если число  $a$  входит делителем в разность чисел  $b$ ,  $c$ , то  $b$  и  $c$  называются **сравнимыми по  $a$** , в противном же случае — **несравнимыми**. Число  $a$  мы назовем **модулем**. Каждое из чисел  $b$ ,  $c$  в первом случае называется **вычетом**, а во втором — **невычетом** другого из них.

Эти обозначения применяются в отношении всех целых, как положительных, так и отрицательных\* чисел; на дробные числа они не распространяются. Так, например,  $-9$  и  $+16$  сравнимы по модулю 5; число  $-7$  является вычетом по модулю 11, но невычетом по модулю 3 числа  $+15$ . Так как нуль делится на любое число, то каждое число следует считать сравнимым с самим собой по любому модулю.

#### 2

Все вычеты заданного числа  $a$  по модулю  $m$  содержатся в формуле  $a + km$ , где  $k$  обозначает произвольное целое число. Из теорем, которые мы установим позднее, более легкие могут быть без труда выведены отсюда; однако всякий сможет с такой же легкостью убедиться в их верности и с первого взгляда.

---

\* Модуль, очевидно, всегда нужно брать по абсолютной величине.

В дальнейшем сравнимость чисел мы будем обозначать знаком  $\equiv$ , а модуль, там где это будет нужно, мы будем добавлять заключенным в скобки:  $-16 \equiv 9 \pmod{5}$ ,  $-7 \equiv 15 \pmod{11}$  \*.

### 3

**Теорема.** Если даны  $m$  последовательных целых чисел

$$a, a + 1, a + 2, \dots, a + m - 1$$

и еще некоторое число  $A$ , то из чисел  $a, a + 1, a + 2, \dots, a + m - 1$  будет сравнимо с  $A$  по модулю  $m$  одно и только одно число.

Именно, если  $(a - A)/m$  есть целое число, то  $a \equiv A$ ; если же оно дробное, то пусть ближайшее большее его целое число (если дробь отрицательна, то ближайшее к ней целое число, меньшее ее по абсолютной величине) равно  $k$ ; тогда  $A + km$  будет лежать между  $a$  и  $a + m$  и потому будет искомым числом. Но очевидно, что все отношения

$$\frac{a - A}{m}, \frac{a + 1 - A}{m}, \frac{a + 2 - A}{m}, \dots$$

лежат между  $k - 1$  и  $k + 1$ ; поэтому среди них не более чем одно может быть целым числом.

### Наименьшие вычеты

#### 4

Таким образом, каждое число обладает вычетом как в ряду чисел  $0, 1, 2, \dots, m - 1$ , так и в ряду  $0, -1, -2, \dots, -(m - 1)$ , причем мы будем их называть наименьшими вычетами. Очевидно, что если  $0$  не является вычетом, то наименьших вычетов всегда имеется два, один положительный и один отрицательный. Если их

---

\* Это обозначение я выбрал вследствие большой аналогии, которая имеется между равенствами и сравнениями. По этой же причине Л е ж а н д р в своем сочинении, ниже часто упоминаемом, сохраняет для сравнений просто знак равенства; однако, во избежание возможных двусмысленностей, я не решился следовать его примеру.

абсолютные величины не равны, то одна из них меньше чем  $m/2$ , в противном же случае обе они равны  $m/2$ . Отсюда следует, что каждое число обладает вычетом, который по абсолютной величине не превосходит половины модуля и называется **абсолютно наименьшим вычетом**.

Например, число  $-13$  по модулю 5 обладает наименьшим положительным вычетом 2 (который одновременно является и абсолютно наименьшим вычетом) и наименьшим отрицательным вычетом  $-3$ . Число  $+5$  по модулю 7 является своим собственным наименьшим положительным вычетом, а  $-2$  является его наименьшим отрицательным и одновременно абсолютно наименьшим вычетом.

## Элементарные теоремы о сравнениях

### 5

После того как мы установили эти обозначения, перечислим те свойства сравнимых чисел, которые непосредственно очевидны.

*Числа, сравнимые по составному модулю, сравнимы также и по каждому его делителю.*

*Если несколько чисел сравнимы с одним и тем же числом по одному и тому же модулю, то они сравнимы (по этому же модулю) между собой.*

В следующих теоремах также предполагается, что модуль остается одним и тем же.

*Сравнимые числа имеют одинаковые, а несравнимые — различные наименьшие вычеты.*

### 6

*Если имеется любое количество чисел  $A, B, C, \dots$  и столько же других чисел  $a, b, c, \dots$ , которые сравнимы с первыми по какому-нибудь модулю, т. е.*

$$A \equiv a, B \equiv b, \dots,$$

*то*

$$A + B + C + \dots \equiv a + b + c + \dots$$

*Если  $A \equiv a, B \equiv b$ , то  $A - B \equiv a - b$ .*



## 7

*Если  $A \equiv a$ , то и  $kA \equiv ka$ .*

Если  $k$  — положительное число, то это есть просто специальный случай теоремы предыдущего пункта, который получается, если положить  $A = B = C = \dots$  и  $a = b = c = \dots$ . Если  $k$  отрицательно, то  $-k$  положительно, поэтому  $-kA \equiv -ka$ , откуда  $kA \equiv ka$ .

*Если  $A \equiv a$ ,  $B \equiv b$ , то также  $AB \equiv ab$ .*

Действительно,  $AB \equiv Ab \equiv ab$ .

## 8

*Если имеется любое количество чисел  $A, B, C, \dots$  и столько же других чисел  $a, b, c, \dots$ , которые сравнимы с первыми, т. е.  $A \equiv a$ ,  $B \equiv b, \dots$ , то и произведения чисел каждого ряда сравнимы между собой, т. е.  $ABC \dots \equiv abc \dots$ .*

Согласно предыдущему пункту,  $AB \equiv ab$ , и по той же причине  $ABC \equiv abc$ ; этим же способом можно присоединить и сколько угодно других сомножителей.

Если все числа  $A, B, C, \dots$  взяты равными, как и соответствующие числа  $a, b, c, \dots$ , то получается следующая теорема.

*Если  $A \equiv a$  и  $k$  — целое положительное число, то  $A^k \equiv a^k$ .*

## 9

*Пусть  $X$  — алгебраическая функция переменной величины  $x$  вида*

$$Ax^a + Bx^b + Cx^c + \dots,$$

*где  $A, B, C, \dots$  обозначают какие-нибудь целые числа, а  $a, b, c, \dots$  — целые неотрицательные числа. Тогда, если переменной  $x$  придавать значения, сравнимые по некоторому модулю, то и получающиеся при этом значения функции  $X$  будут сравнимы между собой.*

Пусть  $f, g$  — сравнимые между собой значения  $x$ . Тогда, согласно предыдущему пункту,  $f^a \equiv g^a$  и  $Af^a \equiv Ag^a$ ; точно так же  $Bf^b \equiv Bg^b$  и т. д. Поэтому  $Af^a + Bf^b + Cf^c + \dots \equiv Ag^a + Bg^b + Cg^c + \dots$ , что и требовалось доказать.

Легко понять, как эта теорема может быть распространена на функции многих переменных.

## 10

Таким образом, если в качестве значений  $x$  брать все следующие одно за другим целые числа, а значения функции  $X$  заменять их наименьшими вычетами, то последние образуют ряд, в котором после интервала из  $m$  членов (где  $m$  обозначает модуль) все время повторяются те же самые члены, т. е. этот ряд будет образован бесконечно много раз повторяющимся периодом из  $m$  членов. Если, например,  $X = x^3 - 8x + 6$  и  $m = 5$ , то для  $x = 0, 1, 2, 3, \dots$  значения  $X$  имеют следующие наименьшие положительные вычеты: 1, 4, 3, 4, 3, 1, 4, ..., где первые пять: 1, 4, 3, 4, 3 повторяются до бесконечности; и если ряд продолжается в обратную сторону, т. е. если  $x$  придаются отрицательные значения, то повторяется тот же самый период с обратным порядком следования членов. Отсюда ясно, что во всем ряду нет никаких других членов, кроме тех, которые образуют этот период.

## 11

В силу сказанного в рассмотренном примере  $X$  не может быть  $\equiv 0$  или  $\equiv 2 \pmod{5}$ , а тем более не может быть  $= 0$  или  $= 2$ . Отсюда следует, что уравнения  $x^3 - 8x + 6 = 0$  и  $x^3 - 8x + 4 = 0$  не разрешимы в целых числах, а вследствие этого, как известно, и в рациональных числах. Вообще очевидно, что если функция  $X$  от неизвестного  $x$  имеет вид

$$x^n + Ax^{n-1} + Bx^{n-2} + \dots + N,$$

где  $A, B, C, \dots$  — целые числа, и  $n$  — целое положительное число, то уравнение  $X = 0$  (к такому виду, как известно, могут быть приведены все алгебраические уравнения) не имеет рациональных корней, если сравнение  $X \equiv 0$  не может удовлетворяться хотя бы по какому-нибудь одному модулю. Этот критерий, который непосредственно очевиден, будет более подробно рассматриваться в разделе VIII. Однако уже сейчас на этом примере можно составить себе некоторое представление о пользе этого исследования.

## Некоторые приложения

## 12

На теоремах, изложенных в этой главе, основывается бóльшая часть того, что обычно принято изучать в арифметике, например, *признаки делимости* заданного числа на 9, 11 и другие числа. *По модулю 9* все числа, являющиеся степенями 10, сравнимы с единицей. Поэтому, если заданное число имеет вид  $a + 10b + 100c + \dots$ , то оно будет давать тот же остаток по модулю 9, что и  $a + b + c + \dots$ . Отсюда следует, что если сложить цифры числа, записанного в десятичной системе, то эта сумма и данное число дают одинаковые наименьшие вычеты, и потому первая может делиться на 9, когда второе делится на 9, и обратно. Так же обстоит дело и для делителя 3. Далее, так как  $100 \equiv 1$  по модулю 11, то всегда  $10^2 \equiv 1$ , а  $10^{2k+1} \equiv 10 \equiv -1$ , и потому число вида  $a + 10b + 100c + \dots$  имеет по модулю 11 тот же наименьший вычет, что и  $a - b + c - \dots$ , откуда сразу получается известное правило. Из этих же принципов легко могут быть выведены все подобные признаки.

Точно так же в вышеизложенном следует искать основу тех правил, которые обычно рекомендуются для *проверки правильности арифметических операций*. Именно, если одно число получается из других посредством сложения, вычитания, умножения или возведения в степень, то вместо заданных чисел подставляются их наименьшие вычеты по некоторому удобному модулю (обычно, 9 или 11, так как вычеты по этим модулям в нашей десятичной системе, как мы уже показали, находятся особенно легко). Получающееся в результате операций число должно быть сравнимо с тем, которое получается после замены чисел их вычетами. Если же этого не случится, то мы заключаем, что в вычисления вкралась ошибка.

Так как, однако, эти и им подобные вопросы достаточно хорошо известны, то было бы излишним дольше на них задерживаться.

---

## РАЗДЕЛ II

### О СРАВНЕНИЯХ ПЕРВОЙ СТЕПЕНИ

#### Предварительные теоремы о простых числах, сомножителях и т. д.

13

**Теорема.** *Произведение двух положительных чисел, каждое из которых меньше заданного простого числа, не может делиться на это простое число.*

Пусть  $p$  — простое число, а  $a$  — положительное число, меньшее  $p$ ; тогда утверждается, что не существует положительного числа  $b < p$ , обладающего тем свойством, что  $ab \equiv 0 \pmod{p}$ .

**Доказательство.** Предположим, что существуют числа  $b, c, d, \dots$ , которые все меньше  $p$  и для которых  $ab \equiv 0, ac \equiv 0, ad \equiv 0, \dots \pmod{p}$ . Из всех этих чисел пусть  $b$  — наименьшее, так что среди чисел, меньших  $p$ , ни одно уже не обладает указанным свойством. Тогда, очевидно,  $b > 1$ . Действительно, если бы было  $b = 1$ , то мы имели бы  $ab = a < p$  (по условию), т. е.  $ab$  не делилось бы на  $p$ . Следовательно,  $p$ , будучи простым числом, не делится на  $b$ , а лежит между некоторыми двумя следующими одно за другим кратными  $b$ , например, между  $tb$  и  $(t+1)b$ . Если  $p - tb = b'$ , то  $b'$  будет положительным числом, меньшим чем  $b$ . Так как, по нашему предположению,  $ab \equiv 0 \pmod{p}$ , то (согласно п. 7) также и  $t ab \equiv 0$ , и потому, вычитая это из  $ap \equiv 0$ , мы получаем  $a(p - tb) = ab' \equiv 0$ , т. е.  $b'$  должно было бы содержаться среди

чисел  $b, c, d, \dots$ , хотя оно меньше, чем наименьшее среди этих чисел число  $b$ . Это приводит к противоречию.

## 14

*Если ни  $a$ , ни  $b$  не делятся на простое число  $p$ , то и произведение  $ab$  не делится на  $p$ .*

Пусть наименьшие положительные вычеты чисел  $a, b$  по модулю  $p$  суть  $\alpha, \beta$ , из которых ни один (по условию) не равен 0. Если бы было  $ab \equiv 0 \pmod{p}$ , то, так как  $ab \equiv \alpha\beta$ , также было бы  $\alpha\beta \equiv 0$ , что противоречит предыдущей теореме.

Доказательство этой теоремы было дано еще Евклидом («Начала», VII, 32). Однако мы не захотели его опустить, во-первых, потому, что в настоящее время часто или вообще пропускают это доказательство, или основывают его на неубедительных соображениях, а, во-вторых, потому что суть примененного здесь метода, который в дальнейшем послужит нам для отыскания значительно более глубоких фактов, легче может быть понята на более простом примере.

## 15

*Если ни одно из чисел  $a, b, c, d, \dots$  не делится на простое число  $p$ , то и произведение  $abcd \dots$  не делится на  $p$ .*

Согласно предыдущему пункту, на  $p$  не делится  $ab$ , а потому — также и  $abc$ , а потому также и  $abcd$  и т. д.

## 16

**Теорема.** *Каждое составное число может быть разложено на простые сомножители только одним единственным образом.*

**Доказательство.** То, что каждое составное число может быть разложено на простые сомножители, известно из основ; однако то, что этого нельзя сделать несколькими различными способами, совершенно необоснованно по большей части предполагается само собой разумеющимся. Если мы предположим, что составное число  $A$ , равное  $a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа, раз-

ложимо на простые сомножители еще и другим способом, то прежде всего ясно, что в этой второй системе сомножителей не может встречаться других простых чисел, кроме  $a, b, c, \dots$ , так как составленное из этих последних число  $A$  не может делиться ни на какое другое простое число. С другой стороны, в этой второй системе сомножителей ни одно из простых чисел  $a, b, c, \dots$  не может отсутствовать, так как иначе (согласно предыдущему пункту) число  $A$  не делилось бы на него. Поэтому оба разложения на множители могут отличаться только тем, что в одно из них какое-нибудь простое число входит большее число раз, чем в другое. Пусть  $p$  такое простое число, которое в одном разложении встречается  $m$  раз, а в другом разложении  $n$  раз, и пусть  $m > n$ . Если теперь из обеих систем выбросить по  $n$  сомножителей, равных  $p$ , то в одной из них еще будет оставаться  $m - n$  сомножителей  $p$ , а в другой их уже не будет совсем, так что для числа  $A/p^n$  мы получим два разложения на множители, из которых одно совсем не содержит сомножителя  $p$ , а другое содержит его  $m - n$  раз. Это, однако, противоречит тому, что мы только что доказали.

## 17

Таким образом, если составное число  $A$  есть произведение чисел  $B, C, D, \dots$ , то ясно, что среди простых сомножителей чисел  $B, C, D, \dots$  не может быть никаких других, кроме тех, которые встречаются среди сомножителей числа  $A$ , и что каждый из этих простых сомножителей должен входить в  $B, C, D, \dots$  в общем столько же раз, сколько и в  $A$ . Отсюда получается критерий, при помощи которого можно узнать, делит ли число  $B$  другое число  $A$ , или нет. Первое имеет место тогда, когда  $B$  не содержит других сомножителей, кроме входящих в  $A$ , а их содержит не большее число раз, чем  $A$ .

Если какое-либо из этих условий не выполняется, то  $B$  не является делителем  $A$ .

При помощи комбинаторики отсюда легко выводится, что если

$$A = a^\alpha b^\beta c^\gamma \dots,$$

где  $a, b, c, \dots$ , как и раньше, обозначают различные простые числа,

то количество различных делителей  $A$ , включая 1 и  $A$ , равно

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

18

Если поэтому  $A = a^\alpha b^\beta c^\gamma \dots$ ,  $K = k^\kappa l^\lambda m^\mu \dots$  и все простые числа  $a, b, c, \dots, k, l, m, \dots$  различны между собой, то  $A$  и  $K$  не имеют общих делителей, кроме 1, т. е. они взаимно просты.

**Наибольший общий делитель** нескольких заданных чисел  $A, B, C, \dots$  находят следующим образом: все эти числа разлагают на простые сомножители, и из них выбирают те, которые являются общими для всех чисел  $A, B, C, \dots$  (если таких нет, то нет и общих делителей). Затем смотрят, сколько раз каждый из этих простых сомножителей содержится по отдельности в каждом из чисел  $A, B, C, \dots$ , т. е. в какой степени каждый входит в числа  $A, B, C, \dots$ . Наконец, для каждого простого сомножителя берут наименьшую из всех степеней, которые он имеет в  $A, B, C, \dots$ , и образуют произведение всех этих степеней; оно и будет искомым наибольшим общим делителем.

Если же мы хотим найти **наименьшее общее кратное** чисел  $A, B, C, \dots$ , то следует поступать так. Нужно взять все простые числа, делящие хотя бы одно из чисел  $A, B, C, \dots$ , затем выбрать для каждого из них наибольшую степень из всех, с которыми оно входит в числа  $A, B, C, \dots$  и образовать произведение всех таким способом выбранных степеней; оно и будет искомым наименьшим общим кратным.

**Пример.** Пусть  $A = 504 = 2^3 \cdot 3^2 \cdot 7$ ,  $B = 2880 = 2^6 \cdot 3^2 \cdot 5$ ,  $C = 864 = 2^5 \cdot 3^3$ . Чтобы найти наибольший общий делитель, мы должны взять простые сомножители 2, 3 в степенях 3, 2, так что этот наибольший общий делитель равен  $2^3 \cdot 3^2 = 72$ . Наименьшее же общее кратное есть  $2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60\,480$ .

Доказательства, ввиду их легкости, мы опускаем. Решение этих вопросов в том случае, когда разложение чисел  $A, B, C, \dots$  на множители не дано, известно из основ.

## 19

*Если числа  $a, b, c, \dots$  взаимно просты с некоторым числом  $k$ , то и их произведение  $abc\dots$  взаимно просто с  $k$ .*

Действительно, так как ни одно из чисел  $a, b, c, \dots$  не имеет с  $k$  общего простого сомножителя, а в произведение  $abc\dots$  могут входить только те простые сомножители, которые являются делителями хотя бы одного из чисел  $a, b, c, \dots$ , то и произведение  $abc\dots$  не имеет с  $k$  общих простых сомножителей. Поэтому, согласно предыдущему пункту,  $k$  и  $abc\dots$  взаимно просты.

*Если числа  $a, b, c, \dots$  попарно взаимно просты и каждое из них делит число  $k$ , то и их произведение есть делитель  $k$ .*

Это тоже легко получается из пп. 17 и 18. Действительно, если  $p$  есть любой простой делитель произведения  $abc\dots$  и содержится в нем  $\pi$  раз, то одно из чисел  $a, b, c, \dots$  должно содержать этот делитель  $\pi$  раз. Поэтому и  $k$ , делящееся на каждое из этих чисел,  $\pi$  раз содержит делителем  $p$ . Аналогично дело обстоит со всеми делителями произведения  $abc\dots$ .

*Поэтому, если два числа  $m, n$  сравнимы между собой по взаимно простым модулям  $a, b, c, \dots$ , то они сравнимы и по их произведению.*

Действительно, так как число  $m - n$  делится на каждое из чисел  $a, b, c, \dots$ , то оно делится и на их произведение.

*Наконец, если  $a$  взаимно просто с  $b$  и  $ak$  делится на  $b$ , то  $k$  должно делиться на  $b$ .*

Действительно, так как число  $ak$  делится на  $a$  и на  $b$ , оно должно делиться на их произведение  $ab$ , т. е.  $\frac{ak}{ab} = \frac{k}{b}$  есть целое число.

## 20

*Если число  $A = a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  — различные простые числа, есть степень некоторого другого числа, скажем,  $A = k^n$ , то все показатели  $\alpha, \beta, \gamma, \dots$  делятся на  $n$ .*

Действительно, число  $k$  не содержит других простых сомножителей, кроме  $a, b, c, \dots$ , а их содержит все. Если сомножитель  $a$  в число  $k$  входит  $\alpha'$  раз, то в  $k^n = A$  он содержится  $n\alpha'$  раз. Поэтому  $n\alpha' = \alpha$  и  $\alpha/n$  есть целое число. Точно так же доказывается, что числа  $\beta/n, \dots$  — целые.



## 21

Если  $a, b, c, \dots$  попарно взаимно просты, а произведение  $abc \dots$  есть некоторая степень, например,  $abc \dots = k^n$ , то каждое из чисел  $a, b, c, \dots$  тоже является  $n$ -й степенью.

Пусть  $a = l^\lambda m^\mu r^\pi$ , где  $l, m, r, \dots$  обозначают различные простые числа, ни одно из которых, согласно предположению, не является делителем чисел  $b, c, \dots$ . Тогда произведение  $abc \dots$  содержит  $\lambda$  раз сомножитель  $l$ ,  $\mu$  раз — сомножитель  $m$  и т. д. Таким образом (согласно предыдущему пункту),  $\lambda, \mu, \pi, \dots$  делятся на  $n$  и потому

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} r^{\frac{\pi}{n}} \dots$$

есть целое число. То же самое имеет место и в отношении чисел  $b, c, \dots$ .

Эти теоремы о простых числах мы должны были предпослать в первую очередь. Теперь мы обращаемся к тем теоремам, которые имеют уже более близкое отношение к поставленной нами цели.

## 22

Если числа  $a, b$  делятся на число  $k$  и сравнимы между собой по взаимно простому с  $k$  модулю  $m$ , то и числа  $a/k$  и  $b/k$  сравнимы между собой по этому же модулю.

Действительно,  $a - b$  делится на  $k$  и, согласно условию, также и на  $m$ ; поэтому (в силу п. 19)  $a - b/k$  делится на  $m$ , т. е.  $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$ .

Если же при тех же самых остальных предположениях  $m$  и  $k$  имеют наибольший общий делитель  $e$ , то  $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$ .

Действительно,  $k/e$  и  $m/e$  взаимно просты. А так как  $(a - b)$  делится как на  $k$ , так и на  $m$ , и потому  $(a - b)/e$  делится на  $k/e$  и на  $m/e$ , а следовательно, и на  $km/e^2$ , то  $(a - b)/k$  делится на  $m/e$ , т. е.  $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$ .

## 23

*Если  $a$  взаимно просто с  $m$ , и  $e, f$  — несравнимые по модулю  $m$  числа, то  $ae$  и  $af$  тоже несравнимы по модулю  $m$ .*

Это есть просто обратная теорема к теореме предыдущего пункта.

Отсюда вытекает, что если  $a$  умножить на все целые числа от 0 до  $m + 1$  и произведения заменить их наименьшими вычетами по модулю  $m$ , то эти последние будут все отличны один от другого. И так как число этих вычетов, которые все меньше  $m$ , равно  $m$ , а чисел от 0 до  $m - 1$  столько же, то, следовательно, ни одно из этих чисел не может отсутствовать среди этих вычетов.

## 24

*Выражение  $ax + b$ , в котором  $a, b$  обозначают данные числа, а  $x$  — неизвестное или переменное число, может быть сделано сравнимым по взаимно простому с  $a$  модулю  $m$  с любым заданным числом.*

Пусть число, которое должно быть сравнимо с указанным выражением, есть  $c$ , а наименьший положительный вычет  $c - b$  по модулю  $m$  есть  $e$ . Тогда, согласно предыдущему пункту, имеется хотя бы одно значение  $x < m$  с тем свойством, что наименьший вычет произведения  $ax$  по модулю  $m$  равен  $e$ . Если это значение есть  $v$ , то  $av \equiv e \equiv c - b$ , и потому  $av + b \equiv c \pmod{m}$ .

## 25

*Выражение, которое, аналогично уравнению, связывает между собой две сравнимые одна с другой величины, мы будем называть сравнением. Сравнение, содержащее неизвестное, называется решенным, если для этого неизвестного найдено удовлетворяющее сравнению значение (корень). Отсюда ясно далее, что понимается под разрешимым или неразрешимым сравнением.*

Наконец, легко видеть, что здесь могут представиться те же различия, что и для уравнений. Дальше встречаются примеры трансцендентных сравнений; алгебраические же сравнения разделяются в зависимости от наивысшей содержащейся в них степени неизве-

стного на сравнения первой, второй и более высоких степеней. Точно так же могут встречаться системы сравнений с несколькими неизвестными, вопрос об исключении которых нам придется рассмотреть.

## Решение сравнений первой степени

### 26

Сравнение первой степени  $ax + b \equiv c$ , согласно п. 24, всегда разрешимо, если модуль взаимно прост с  $a$ . Если  $v$  — подходящее значение  $x$ , т. е. корень сравнения, то, очевидно, что корнями являются и все числа, сравнимые с  $v$  по модулю этого сравнения (п. 9). Обратно, легко видеть, что все корни  $v$  должны быть сравнимы между собой; действительно, если  $t$  — другой корень, то  $av + b \equiv at + b$ , и потому  $av \equiv at$ , откуда  $v \equiv t$  (п. 22). Отсюда следует, что сравнение  $x \equiv v \pmod{m}$  представляет собой полное решение сравнения  $ax + b \equiv c$ .

Так как решения сравнения, которые сравнимы с  $x$ , находятся в нашем распоряжении и в этом отношении сравнимые числа следует рассматривать как эквивалентные, то мы все такие решения сравнения будем считать за одно решение. Поэтому если наше сравнение  $ax + b \equiv c$  не допускает других решений, то мы будем говорить, что оно разрешимо единственным образом, или имеет только один корень. Так, например, сравнение  $6x + 5 \equiv 13 \pmod{11}$  не обладает другими корнями, кроме тех, которые  $\equiv 5 \pmod{11}$ . По иному обстоит дело для сравнений более высоких степеней или для сравнений первой степени, в которых неизвестное умножается на число, не взаимно простое с модулем.

### 27

Остается еще добавить кое-что о нахождении решения сравнения такого рода.

Сначала заметим, что сравнение  $ax + t \equiv u$ , модуль которого предполагается взаимно простым с  $a$ , связано со сравнением  $ax \equiv \pm 1$ . Действительно, если последнему удовлетворяет  $x \equiv r$ , то первое удовлетворяется посредством  $x \equiv \pm (u - t)r$ . Но, если

мы обозначим модуль через  $b$ , то сравнение  $ax \equiv \pm 1$  эквивалентно неопределенному уравнению  $ax = by \pm 1$ , а как такое уравнение надо решать, в настоящее время достаточно хорошо известно. Мы удовольствуемся поэтому тем, что изложим здесь алгоритм вычислений.

Если величины  $A, B, C, D, E, \dots$  так зависят от величин  $\alpha, \beta, \gamma, \delta, \varepsilon, \dots$ , что

$$A = \alpha, B = \beta A + 1, C = \gamma B + A, D = \delta C + B, E = \varepsilon D + C, \dots,$$

то мы будем для краткости обозначать их следующим образом:

$$A = [\alpha], B = [\alpha, \beta], C = [\alpha, \beta, \gamma], D = [\alpha, \beta, \gamma, \delta], \dots^*.$$

Пусть теперь дано неопределенное уравнение  $ax = by \pm 1$ , в котором  $a, b$  положительны. Мы предположим, что  $a$  не меньше, чем  $b$ ; это позволительно. Тогда по образцу известного алгоритма для отыскания наибольшего общего делителя двух чисел мы посредством обыкновенного деления образуем равенства

$$a = \alpha b + c, b = \beta c + d, c = \gamma d + e, \dots,$$

в которых  $\alpha, \beta, \gamma, \dots, c, d, e, \dots$  суть целые положительные числа и  $b, c, d, e, \dots$  все время убывают, до тех пор, пока не придем к равенству вида

$$m = \mu n + 1,$$

---

\* Это взаимоотношение величин может быть рассмотрено с намного более общей точки зрения, что мы при случае, возможно, и сделаем. Здесь же мы лишь добавим две теоремы, которые найдут применение в настоящих исследованиях, именно:

$$(1) \quad [\alpha, \beta, \gamma, \dots, \lambda, \mu] \cdot [\beta, \gamma, \dots, \lambda] - \\ - [\alpha, \beta, \gamma, \dots, \lambda] \cdot [\beta, \gamma, \dots, \lambda, \mu] = \pm 1,$$

где нужно брать верхний или нижний знак в зависимости от того, четно количество чисел  $\alpha, \beta, \gamma, \dots, \lambda, \mu$  или нечетно.

(2) Последовательность чисел  $\alpha, \beta, \gamma, \dots$  можно обратить, т. е.

$$[\alpha, \beta, \gamma, \dots, \lambda, \mu] = [\mu, \lambda, \dots, \gamma, \beta, \alpha].$$

Доказательства не трудны, поэтому мы их опускаем.

что, как известно, всегда случится. Тогда

$$a = [n, \mu, \dots, \gamma, \beta, \alpha], \quad b = [n, \mu, \dots, \gamma, \beta].$$

Поэтому, если взять

$$x = [\mu, \dots, \gamma, \beta], \quad y = [\mu, \dots, \gamma, \beta, \alpha],$$

то будет иметь место  $ax = by + 1$ , когда количество чисел  $\alpha, \beta, \gamma, \dots, \mu, n$  четно, и  $ax = by - 1$ , когда оно нечетно.

## 28

Общее решение таких неопределенных уравнений сначала изучал Э й л е р, «*Comment. Petrop.*», Т. VII, р. 46 \*. Метод, которым он пользовался, состоит в подстановке вместо  $x, y$  других неизвестных, и в настоящее время хорошо известен. Л а г р а н ж подходил к вопросу несколько по-иному. Именно, из теории непрерывных дробей известно, что если дробь  $a/b$  разложить в непрерывную дробь

$$\frac{1}{\alpha + \frac{1}{\beta + \frac{1}{\gamma + \dots + \frac{1}{\mu + \frac{1}{n}}}}}$$

и, отбросив в ней последний член  $1/n$ , снова превратить ее в обыкновенную дробь  $x/y$ , то будет иметь место  $ax = by \pm 1$ , если  $a$  взаимно просто с  $b$ . Впрочем, оба метода приводят к одному и тому же алгоритму. Исследования Л а г р а н ж а находятся в «*Hist. de l'Ac. de Berlin*», Année 1767, р. 175, и кроме того, в дополнениях к французскому переводу «Алгебры» Э й л е р а.

## 29

Сравнение  $ax + t \equiv u$ , модуль которого не взаимно прост с  $a$  легко может быть сведено к предыдущему случаю. Пусть  $m$  — модуль, и  $\delta$  — наибольший общий делитель чисел  $a, m$ . Прежде всего

\* Ср. дополнения в конце «Исследований».

ясно, что каждое значение  $x$ , удовлетворяющее сравнению по модулю  $m$ , удовлетворяет и тому же сравнению по модулю  $\delta$  (п. 5). Но так как  $\delta$  есть делитель  $a$ , всегда имеет место  $ax \equiv 0 \pmod{\delta}$ . Поэтому заданное сравнение разрешимо только тогда, когда  $t \equiv u \pmod{\delta}$ , т. е. когда  $t - u$  делится на  $\delta$ .

Таким образом, если мы положим  $a = \delta e$ ,  $m = \delta f$ ,  $t - u = \delta k$ , то  $e$  будет взаимно просто с  $f$ , и сравнению  $\delta ex + \delta k \equiv 0 \pmod{\delta f}$  будет эквивалентно сравнение  $ex + k \equiv 0 \pmod{f}$ , т. е. каждое значение  $x$ , которое удовлетворяет последнему, будет удовлетворять также и первому, и обратно. Действительно,  $ex + k$  может, очевидно, делиться на  $f$  только тогда, когда  $\delta ex + \delta k$  делится на  $\delta f$ , и обратно. Но сравнение  $ex + k \equiv 0 \pmod{f}$  мы уже выше научились решать, и мы получаем, что если  $v$  есть одно из значений  $x$ , то  $x \equiv v \pmod{f}$  представляет полное решение заданного сравнения.

### 30

*В случае составного модуля иногда лучше применять следующий метод.*

Пусть модуль  $= mn$ , и заданное сравнение есть  $ax \equiv b$ . Решим сначала это сравнение по модулю  $m$ , и предположим, что оно удовлетворяется, если  $x \equiv v \pmod{m/\delta}$ , где  $\delta$  обозначает наибольший общий делитель чисел  $m$  и  $a$ . Тогда ясно, что каждое значение  $x$ , удовлетворяющее сравнению  $ax \equiv b$  по модулю  $mn$  должно удовлетворять и сравнению по модулю  $m$ , и потому должно представляться в виде  $v + \frac{m}{\delta} x'$ , где  $x'$  обозначает неизвестное число, хотя обратное неверно, т. е. не все числа, представимые в виде  $v + \frac{m}{\delta} x'$ , удовлетворяют сравнению по модулю  $mn$ . Но если надо найти такое  $x$ , что  $v + \frac{m}{\delta} x'$  является корнем сравнения  $ax \equiv b \pmod{mn}$ , то его можно получить, решая сравнение  $\frac{am}{\delta} x' + av \equiv b \pmod{mn}$ , которое эквивалентно сравнению  $\frac{a}{\delta} x' \equiv \frac{b - av}{m} \pmod{n}$ . Из этого следует, что решение любого сравнения первой степени по модулю  $mn$  сводится к решению двух сравнений по модулям  $m$  и  $n$ . Легко видеть, что если  $n$  снова есть произведение двух

сомножителей, то решение сравнения по модулю  $n$  зависит от решения двух сравнений, модули которых являются его сомножителями. Вообще решение сравнения по любому составному модулю зависит от решений других сравнений, модули которых являются его сомножителями. Последние же, когда это целесообразно, могут предполагаться простыми числами.

**Пример.** Если дано сравнение  $19x \equiv 1 \pmod{140}$ , то надо решить его сначала по модулю 2, откуда получается  $x \equiv 1 \pmod{2}$ . Если положить  $x = 1 + 2x'$ , то получается сравнение  $38x' \equiv -18 \pmod{140}$ , которое эквивалентно сравнению  $19x' \equiv -9 \pmod{70}$ . Если последнее снова решить по модулю 2, то получится  $x' \equiv 1 \pmod{2}$ , и потому, если положить  $x' = 1 + 2x''$ ,  $38x'' \equiv -28 \pmod{70}$  или  $19x'' \equiv -14 \pmod{35}$ . Последнее, решенное по модулю 5, дает  $x'' \equiv 4 \pmod{5}$ , и если положить  $x'' = 4 + 5x'''$ , то  $95x''' \equiv -90 \pmod{35}$  или  $19x''' \equiv -18 \pmod{7}$ . Наконец, из последнего сравнения следует  $x''' \equiv 2 \pmod{7}$ , и если положить  $x''' = 2 + 7x''''$ , то получится  $x = 59 + 140x''''$ . Поэтому полным решением заданного сравнения является  $x \equiv 59 \pmod{140}$ .

### 31

Подобно тому, как корень уравнения  $ax = b$  выражается в виде  $b/a$ , мы будем также и корень сравнения  $ax \equiv b$  обозначать через  $b/a$  и для ясности приписывать модуль. Так, например,  $\frac{19}{17} \pmod{12}$  обозначает всякое число, которое  $\equiv 11 \pmod{12}$  [что по аналогии может быть также обозначено через  $\frac{11}{1} \pmod{12}$ ]. Вообще, из предыдущего вытекает, что  $\frac{b}{a} \pmod{c}$  не имеет вещественного значения (или, если так говорить больше нравится, является мнимым выражением), если  $a$  и  $c$  имеют общий делитель, который в то же время не делит  $b$ . За исключением этого случая выражение  $\frac{b}{a} \pmod{c}$  всегда имеет вещественные значения, и притом бесконечно много; однако все они сравнимы между собой по модулю  $c$ , если  $a$  взаимно просто с  $c$ , или по модулю  $c/\delta$ , если  $\delta$  есть наибольший общий делитель чисел  $c$  и  $a$ .

С этими выражениями можно оперировать почти так же, как с обычными дробями. Некоторые свойства, которые легко могут быть выведены из предыдущего, мы здесь укажем.

1. Если по модулю  $c$  имеет место  $a \equiv \alpha$ ,  $b \equiv \beta$ , то выражения  $\frac{a}{b} \pmod{c}$  и  $\frac{\alpha}{\beta} \pmod{c}$  эквивалентны.

2.  $\frac{a\delta}{b\delta} \pmod{c\delta}$  эквивалентно  $\frac{a}{b} \pmod{c}$ .

3.  $\frac{ak}{bk} \pmod{c}$  эквивалентно  $\frac{a}{b} \pmod{c}$ , если  $k$  взаимно просто с  $c$ .

Мы могли бы привести еще много подобных теорем; так как, однако, они не связаны ни с какими трудностями и не очень нужны для дальнейшего, мы переходим к несколько иным вещам.

### Нахождение числа, которое сравнимо с заданными вычетами по заданным модулям

#### 32

При помощи изложенного выше легко может быть решена следующая задача, которая часто будет встречаться в дальнейшем: *найти все числа, которые имеют заданные вычеты по заданным в любом количестве модулям.* Пусть сначала даны два модуля  $A$  и  $B$ , по которым искомое число  $z$  должно быть сравнимо соответственно с  $a$  и  $b$ . Тогда все значения  $z$  содержатся в выражении  $Ax + a$ , где  $x$  — неизвестное число, с тем, однако, свойством, что  $Ax + a \equiv b \pmod{B}$ . Если  $\delta$  есть наибольший общий делитель чисел  $A$  и  $B$ , то полное решение этого сравнения будет иметь вид  $x \equiv v \pmod{\frac{B}{\delta}}$ , или, что то же самое,  $x = v + \frac{kB}{\delta}$ , где  $k$  обозначает произвольное целое число. Поэтому формула  $Av + a + \frac{kAB}{\delta}$  охватывает все значения  $z$ , т. е.  $z \equiv Av + a \pmod{\frac{AB}{\delta}}$  представляет собой полное решение вопроса.

Если к  $A$  и  $B$  добавлен еще третий модуль  $C$ , по которому искомое число  $z$  должно быть сравнимо с  $c$ , то нужно дальше рассуждать таким же образом, ибо первые два условия уже объединены в одно. Если  $\varepsilon$  есть наибольший общий делитель чисел  $AB/\delta$



и  $C$ , и  $x \equiv w \pmod{\frac{C}{\varepsilon}}$  есть решение сравнения  $\frac{AB}{\delta} x + Av + a \equiv \equiv c \pmod{C}$ , то полное решение задачи дается сравнением  $z \equiv \frac{ABw}{\delta} + + Av + a \pmod{\frac{ABC}{\delta\varepsilon}}$ . Подобным же образом следует поступать и в случае, когда задано большее число модулей. Заметим, что  $AB/\delta$ ,  $ABC/\delta\varepsilon$  суть наименьшие общие кратные соответственно чисел  $A$ ,  $B$  и  $A$ ,  $B$ ,  $C$ . Отсюда легко усмотреть, что сколько бы ни было задано модулей  $A$ ,  $B$ ,  $C$ , ..., полное решение будет иметь вид  $z \equiv r \pmod{M}$ , где  $M$  есть наименьшее общее кратное этих чисел.

Далее, если какое-нибудь из вспомогательных сравнений неразрешимо, то из этого следует, что и решение всей задачи невозможно. Это, однако, не может случиться, если все числа  $A$ ,  $B$ ,  $C$ , ... между собой взаимно просты.

**Пример.** Пусть числа  $A$ ,  $B$ ,  $C$ ;  $a$ ,  $b$ ,  $c$  суть соответственно, 504, 35, 16; 17, —4, 33. Здесь два условия, а именно,

$$z \equiv 17 \pmod{504} \text{ и } \equiv -4 \pmod{35}$$

эквивалентны одному:  $z \equiv 521 \pmod{2520}$ . Последнее же, объединенное с условием  $z \equiv 33 \pmod{16}$ , дает  $z \equiv 3041 \pmod{5040}$ .

### 33

Если все числа  $A$ ,  $B$ ,  $C$ , ... взаимно просты, то их произведение является, как известно, их наименьшим общим кратным. В этом случае все сравнения  $z \equiv a \pmod{A}$ ,  $z \equiv b \pmod{B}$ , ... эквивалентны одному сравнению  $z \equiv r \pmod{R}$ , в котором  $R$  обозначает произведение чисел  $A$ ,  $B$ ,  $C$ , ... Отсюда следует, что, и наоборот, одно условие  $z \equiv r \pmod{R}$  может быть разложено на несколько. Именно, если  $R$  каким-нибудь образом разложено на взаимно простые сомножители  $A$ ,  $B$ ,  $C$ , ..., то условиями  $z \equiv r \pmod{A}$ ,  $z \equiv r \pmod{B}$ ,  $z \equiv r \pmod{C}$ , ... исходное условие полностью исчерпывается. Это замечание открывает нам путь к тому, чтобы не только сразу узнавать о невозможности решения задачи в случае, когда это вытекает из заданных условий, но чтобы также проводить вычисления короче и удобнее.

Пусть, как и раньше, заданные условия суть  $z \equiv a \pmod{A}$ ,  $z \equiv b \pmod{B}$ ,  $z \equiv c \pmod{C}$ , .... Разложим все модули на взаимно простые сомножители,  $A$  — на  $A'A''A'''...$ ,  $B$  — на  $B'B''B'''...$  и т. д., причем так, что числа  $A'$ ,  $A''$ , ...,  $B'$ ,  $B''$ , ... либо простые, либо являются степенями простых чисел. Таким образом, если одно из чисел  $A$ ,  $B$ ,  $C$ , ... само является или простым числом, или степенью такового, то его раскладывать на множители не нужно. Тогда из предыдущего получается, что заданные условия можно заменить следующими:

$$z \equiv a \pmod{A'}, \quad z \equiv a \pmod{A''}, \quad z \equiv a \pmod{A'''}, \quad \dots,$$

$$z \equiv b \pmod{B'}, \quad z \equiv b \pmod{B''}, \quad z \equiv b \pmod{B'''}, \quad \dots$$

и т. д.

Если бы числа  $A$ ,  $B$ ,  $C$ , ... не были все попарно взаимно просты, например,  $A$  не было бы взаимно просто с  $B$ , то, очевидно, простые делители чисел  $A$  и  $B$  не могли бы быть все различны между собой, и потому среди сомножителей  $A'$ ,  $A''$ ,  $A'''$ , ... имелся бы такой, для которого среди сомножителей  $B'$ ,  $B''$ ,  $B'''$ , ... нашелся бы или равный ему, или кратный ему, или делящий его. Если  $A' = B'$ , то условия  $z \equiv a \pmod{A'}$  и  $z \equiv b \pmod{B'}$  должны быть идентичными, т. е.  $a \equiv b \pmod{A'}$  или  $B'$ , так что одно из этих условий можно отбросить. Если  $a \not\equiv b \pmod{A'}$ , то решение задачи невозможно. Если же  $B'$  кратно  $A'$ , то условие  $z \equiv a \pmod{A'}$  должно содержаться в условии  $z \equiv b \pmod{B'}$ , т. е. вытекающее из последнего условие  $z \equiv b \pmod{A'}$  должно быть идентично первому. Отсюда следует, что условие  $z \equiv a \pmod{A'}$ , если оно не противоречит другим (в противном случае решения нет), может быть отброшено. Если выбросить таким способом все лишние условия, то очевидно, что те из модулей  $A'$ ,  $A''$ ,  $A'''$ , ...,  $B'$ ,  $B''$ ,  $B'''$ , ..., которые после этого останутся, будут взаимно просты. Мы можем тогда быть уверенными в возможности решения задачи и можем применять указанные выше правила.

## 35

**Пример.** Если, как и выше, должно быть  $z \equiv 17 \pmod{504}$ ,  $\equiv -4 \pmod{35}$  и  $\equiv 33 \pmod{16}$ , то эти условия могут быть разложены на следующие:

$$\begin{aligned} z &\equiv 17 \pmod{8}, \equiv 17 \pmod{9}, \equiv 17 \pmod{7}; \\ z &\equiv -4 \pmod{5}, \equiv -4 \pmod{7}; \\ z &\equiv 33 \pmod{16}. \end{aligned}$$

Из них можно отбросить условия  $z \equiv 17 \pmod{8}$  и  $z \equiv 17 \pmod{7}$ , так как первое содержится в условии  $z \equiv 33 \pmod{16}$ , а второе идентично с  $z \equiv -4 \pmod{7}$ . Поэтому остаются следующие условия:

$$z \equiv \begin{cases} 17 \pmod{9}, \\ -4 \pmod{5}, \\ -4 \pmod{7}, \\ 33 \pmod{16}, \end{cases}$$

из которых следует  $z \equiv 3041 \pmod{5040}$ .

Отметим еще, что в большинстве случаев удобнее снова объединить те из оставшихся условий, которые получились из одного и того же первоначального условия. Например, если некоторые из условий  $z \equiv a \pmod{A'}$ ,  $z \equiv a \pmod{A''}$ , ... отброшены, то составленное из остальных условие будет состоять в том, что  $y \equiv a$  по модулю, который равен произведению оставшихся модулей из числа  $A'$ ,  $A''$ ,  $A'''$ , ... Так, в нашем примере из условий  $z \equiv -4 \pmod{5}$ ,  $z \equiv -4 \pmod{7}$  снова получается то условие, из которого они возникли, именно,  $z \equiv -4 \pmod{35}$ . Далее, отсюда следует, что в отношении краткости вычислений не совсем безразлично, какое из совпадающих условий отбрасывать; однако в наши намерения не входит вдаваться здесь подробнее в практические приемы, которые лучше усваиваются во время работы, чем по готовым рецептам.

## 36

Если все модули  $A$ ,  $B$ ,  $C$ ,  $D$ , ... взаимно просты, то часто бывает лучше использовать следующий метод. Нужно определить число  $\alpha$ , которое сравнимо с единицей по  $A$  и с нулем по произ-

ведению остальных модулей; пусть  $\alpha$  — любое значение (в большинстве случаев удобнее всего брать среди них *наименьшее*) умноженного на  $BCD \dots$  выражения  $1/BCD \dots \pmod{A}$  (см. п. 32). Точно так же, пусть  $\beta \equiv 1 \pmod{B}$  и  $\equiv 0 \pmod{ACD \dots}$ ,  $\gamma \equiv 1 \pmod{C}$  и  $\equiv 0 \pmod{ABD \dots}$  и т. д. Тогда, если ищется число  $z$ , которое по модулям  $A, B, C, D, \dots$  сравнимо соответственно с  $a, b, c, d, \dots$ , то можно положить

$$z \equiv \alpha a + \beta b + \gamma c + \delta d + \dots \pmod{ABCD \dots}.$$

В самом деле, очевидно, что  $\alpha a \equiv a \pmod{A}$ , в то время как остальные члены  $\beta b, \gamma c, \dots$  все  $\equiv 0 \pmod{A}$ ; поэтому  $z \equiv a \pmod{A}$ . Аналогично и доказательство для других модулей. Такое решение следует предпочесть указанным ранее, если нужно решить несколько задач, в которых модули  $A, B, C, \dots$  сохраняют одни и те же значения; действительно, тогда остаются неизменными и значения чисел  $\alpha, \beta, \gamma, \dots$ . С подобным положением мы сталкиваемся в одном вопросе, связанном с исчислением времени; спрашивается, на какой год в юлианском периоде приходится заданное Рёмеровское число, золотое число и солнечный круг. Здесь  $A = 15$ ,  $B = 19$ ,  $C = 28$ . Так как значение выражения  $1/19 \cdot 28 \pmod{15}$  или  $1/532 \pmod{15}$  равно 13, то  $\alpha = 6916$ . Аналогично находим, что  $\beta = 4200$  и  $\gamma = 4845$ . Поэтому искомое число есть наименьший вычет числа  $6916a + 4200b + 4845c$ , где  $a$  — Рёмеровское число,  $b$  — золотое число и  $c$  — солнечный круг.

### Линейные сравнения со многими неизвестными

#### 37

Предыдущее относилось к сравнениям первой степени с одним неизвестным. Но мы должны еще рассмотреть и сравнения, в которые входит несколько неизвестных. Однако, если бы мы захотели с полной строгостью разобрать все частности вопроса, то нам пришлось бы вдаваться в этом разделе в слишком большое число подробностей, и кроме того, наша задача состоит сейчас не в том, чтобы дать исчерпывающее изложение, а в том, чтобы лишь отметить вопросы,

наиболее достойные внимания; поэтому мы ограничим здесь наше исследование немногими замечаниями, а подробное рассмотрение этого предмета отложим до другого случая.

1. Аналогично тому, как для уравнений, мы можем убедиться, что и здесь мы должны иметь столько сравнений, сколько неизвестных надо определить.

2. Пусть, таким образом, дано столько же сравнений

$$\begin{array}{ll} (A) & ax + by + cz + \dots \equiv f \pmod{m}, \\ (A') & a'x + b'y + c'z + \dots \equiv f', \\ (A'') & a''x + b''y + c''z + \dots \equiv f'', \\ & \dots \dots \dots \end{array}$$

сколько имеется неизвестных  $x, y, z, \dots$

Определим теперь числа  $\xi, \xi', \xi'', \dots$  из уравнений

$$\begin{array}{l} b\xi + b'\xi' + b''\xi'' + \dots = 0, \\ c\xi + c'\xi' + c''\xi'' + \dots = 0 \\ \dots \dots \dots \end{array}$$

и притом так, что все эти числа целые и не имеют общего делителя, что, как известно из теории линейных уравнений, всегда возможно. Подобным же образом определяем числа  $\eta, \eta', \eta'', \dots, \zeta, \zeta', \zeta'', \dots$  из уравнений

$$\begin{array}{l} a\eta + a'\eta' + a''\eta'' + \dots = 0, \\ c\eta + c'\eta' + c''\eta'' + \dots = 0, \\ \dots \dots \dots \\ a\zeta + a'\zeta' + a''\zeta'' + \dots = 0, \\ b\zeta + b'\zeta' + b''\zeta'' + \dots = 0. \\ \dots \dots \dots \end{array}$$

3. Если сравнения  $A, A', A'', \dots$  умножить соответственно сначала на  $\xi, \xi', \xi'', \dots$ , потом на  $\eta, \eta', \eta'', \dots$  и т. д. и затем произведения сложить, получатся, очевидно, следующие сравнения:

$$\begin{array}{l} (a\xi + a'\xi' + a''\xi'' + \dots) x \equiv f\xi + f'\xi' + f''\xi'' + \dots, \\ (b\eta + b'\eta' + b''\eta'' + \dots) y \equiv f\eta + f'\eta' + f''\eta'' + \dots, \\ (c\zeta + c'\zeta' + c''\zeta'' + \dots) z \equiv f\zeta + f'\zeta' + f''\zeta'' + \dots, \\ \dots \dots \dots \end{array}$$

которые мы для краткости представим следующим образом:

$$\sum (a\xi) x \equiv \sum (f\xi), \quad \sum (b\eta) y \equiv \sum (f\eta), \quad \sum (c\zeta) z \equiv \sum (f\zeta), \dots$$

4. Теперь нужно различать *несколько случаев*.

*Во-первых*, если все коэффициенты  $\sum (a\xi), \sum (b\eta), \dots$  при неизвестных взаимно просты с модулем сравнения  $m$ , то эти сравнения можно решить по указанным выше правилам, и полное решение вопроса будет представляться сравнениями вида

$$x \equiv p \pmod{m}, \quad y \equiv q \pmod{m}, \dots^*$$

Если, например, заданы сравнения

$$x + 3y + z \equiv 1 \pmod{8},$$

$$4x + y + 5z \equiv 7,$$

$$2x + 2y + z \equiv 3,$$

то мы находим  $\xi = 9, \xi' = 1, \xi'' = -14$ ; отсюда  $-15x \equiv -26$  и потому  $x \equiv 6 \pmod{8}$ . Таким же образом находим  $15y \equiv -4, 15z \equiv 1$ , откуда  $y \equiv 4, z \equiv 7 \pmod{8}$ .

5. *Во-вторых*, если не все коэффициенты  $\sum (a\xi), \sum (b\eta), \dots$  взаимно просты с модулем, то пусть  $\alpha, \beta, \gamma, \dots$  суть наибольшие общие делители  $m$  и, соответственно,  $\sum (a\xi), \sum (b\eta), \sum (c\zeta), \dots$ . Тогда задача, очевидно, неразрешима, если они не являются одновременно также и делителями соответственно чисел  $\sum (f\xi), \sum (f\eta), \sum (f\zeta), \dots$ . Если же эти условия выполняются, то полное решение сравнений в (3) дается сравнениями вида  $x \equiv p \pmod{\frac{m}{\alpha}}, y \equiv q \pmod{\frac{m}{\beta}}, z \equiv r \pmod{\frac{m}{\gamma}}, \dots$ , или, другими словами, существует  $\alpha$  различных (т. е. несравнимых по модулю  $m$ , таких, как  $p, p + \frac{m}{\alpha}, \dots, p + \frac{(\alpha-1)m}{\alpha}$ ) значений  $x, \beta$  различных значений  $y$ , и т. д., которые удовлетворяют указанным сравнениям; очевидно, что все решения заданных

---

\* Это утверждение, как можно заметить, нуждается в доказательстве, которое мы здесь опустили. В самом деле, из наших рассуждений следует только то, что заданные сравнения не удовлетворяются при других значениях неизвестных  $x, y, z, \dots$ ; а то, что указанные нами значения этим сравнениям удовлетворяют, ниоткуда не следует. Именно, эти сравнения могли бы, вообще говоря, не иметь никаких решений. Подобный же паралогизм часто встречается и в теории линейных уравнений.

сравнений (если они вообще существуют) содержатся здесь. Однако обратить это утверждение нельзя; действительно, в большинстве случаев не все комбинации всевозможных значений  $x$  со всевозможными значениями  $y$ , всевозможными значениями  $z$  и т. д. дают решение задачи, а лишь некоторые из них, которые удовлетворяют одному или нескольким условиям сравнимости. Так как, однако, полное решение этого вопроса не является необходимым для дальнейшего, мы не будем здесь более подробно его исследовать, и удовлетворимся тем, что продемонстрируем положение ведущей на примере.

Пусть заданные сравнения суть

$$3x + 5y + z \equiv 4, \quad 2x + 3y + 2z \equiv 7, \quad 5x + y + 3z \equiv 6 \pmod{12}.$$

Здесь числа  $\xi, \xi', \xi''; \eta, \eta', \eta''; \zeta, \zeta', \zeta''$  равны соответственно 1, —2, 1; 1, 1, —1; —13, 22, —1, откуда вытекает  $4x \equiv -4$ ,  $7y \equiv 5$ ,  $28z \equiv 96$ . Отсюда получаются четыре значения для  $x$ , именно,  $x \equiv 2, 5, 8, 11$ , одно значение для  $y$ , именно  $y \equiv 11$ , четыре значения для  $z$ , именно  $z \equiv 0, 3, 6, 9 \pmod{12}$ . Чтобы теперь узнать, какие комбинации значений  $x$  и значений  $z$  мы имеем право брать, подставим в заданные сравнения вместо  $x, y, z$  соответственно  $2 + 3t, 11, 3u$ , после чего они перейдут в следующие сравнения:

$$57 + 9t + 3u \equiv 0, \quad 30 + 6t + 6u \equiv 0, \quad 15 + 15t + 9u \equiv 0 \pmod{12},$$

а они, как легко видеть, эквивалентны следующим:

$$19 + 3t + u \equiv 0, \quad 10 + 2t + 2u \equiv 0, \quad 5 + 5t + 3u \equiv 0 \pmod{4}.$$

В силу первого из них должно быть  $u \equiv t + 1 \pmod{4}$ ; если мы подставим это значение в два других сравнения, то увидим, что оба они тоже удовлетворяются. Отсюда следует, что значения  $x \equiv 2, 5, 8, 11$  (которые получаются, если положить  $t = 0, 1, 2, 3$ ) необходимо должны комбинироваться соответственно со значениями  $z \equiv 3, 6, 9, 0$ , так что всего мы имеем четыре решения, именно

$$x \equiv 2, 5, 8, 11 \pmod{12};$$

$$y \equiv 11, 11, 11, 11;$$

$$z \equiv 3, 6, 9, 0.$$

К этим исследованиям, благодаря которым мы уже достигли цели этого раздела, мы добавим еще несколько основанных на подобных же принципах теорем, которые мы часто будем использовать впоследствии.

## Различные теоремы

### 38

**Задача.** Требуется узнать, сколько существует положительных чисел, которые меньше данного положительного числа  $A$  и одновременно взаимно просты с ним.

Если количество положительных чисел, которые меньше заданного числа и одновременно взаимно просты с ним, обозначать буквой  $\varphi$ , ставящейся перед числом, то нам нужно найти  $\varphi(A)$ .

I. Если число  $A$  простое, то все числа от 1 до  $A - 1$ , очевидно, взаимно просты с  $A$ ; следовательно, в этом случае

$$\varphi(A) = A - 1.$$

II. Если  $A$  есть степень простого числа, именно,  $A = p^m$ , то взаимно простыми с  $A$  будут все числа, за исключением делящихся на  $p$ . Поэтому из  $p^m - 1$  чисел отбрасываются следующие:  $p, 2p, 3p, \dots, (p^{m-1} - 1)p$ ; таким образом, остается  $p^m - 1 - (p^{m-1} - 1)$  или  $p^m - p^{m-1}$  чисел, так что  $\varphi(p^m) = p^m - p^{m-1}$ .

III. Остальные случаи легко могут быть сведены к двум первым при помощи следующей теоремы.

Если  $A$  разлагается на взаимно простые сомножители  $M, N, P, \dots$ , то

$$\varphi(A) = \varphi(M) \cdot \varphi(N) \cdot \varphi(P) \dots$$

Доказывается это следующим образом. Пусть  $m, m', m'', \dots$  суть числа, которые взаимно просты с  $M$  и меньше чем  $M$ ; количество их, таким образом, равно  $\varphi(M)$ . Точно так же пусть  $n, n', n'', \dots$ , соответственно  $p, p', p'', \dots$  — числа, которые взаимно просты с  $N$ , соответственно с  $P$ , и меньше, чем  $N$ , соответственно, чем  $P$ , количество которых равно  $\varphi(N)$ , соответственно  $\varphi(P)$ , и т. д. Тогда,



как известно, все числа, взаимно простые с произведением  $A$ , взаимно просты также и с отдельными сомножителями  $M, N, P, \dots$ , и обратно (п. 19). Далее, все числа, которые сравнимы по модулю  $M$  с одним из чисел  $m, m', m'', \dots$ , взаимно просты с  $M$  и обратно; то же самое имеет место относительно  $N, P, \dots$ . Поэтому задача сводится к следующей: определить, сколько среди чисел, меньших  $A$ , имеется таких, которые сравнимы с одним из чисел  $m, m', m'', \dots$  по модулю  $M$ , с одним из чисел  $n, n', n'', \dots$  по модулю  $N$  и т. д. Но из п. 32 следует, что все числа, которые имеют по отдельным модулям  $M, N, P, \dots$  одни и те же вычеты, сравнимы по их произведению  $A$ , и что поэтому среди чисел, меньших  $A$ , имеется одно единственное, которое сравнимо с заданными вычетами по отдельным модулям  $M, N, P, \dots$ . Следовательно, искомого числа будет равно количеству всех комбинаций отдельных значений  $m, m', m'', \dots$  с отдельными значениями  $n, n', n'', \dots$ , отдельными значениями  $p, p', p'', \dots$  и т. д. Но как известно из комбинаторики, это количество равно

$$\varphi(M) \cdot \varphi(N) \cdot \varphi(P) \dots$$

IV. Легко видеть, как это применяется к рассматриваемому случаю. Если  $A$  разложено на простые сомножители, т. е. задано в виде  $a^\alpha b^\beta c^\gamma, \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа, то

$\varphi(A) = \varphi(a^\alpha) \cdot \varphi(b^\beta) \cdot \varphi(c^\gamma) \dots = a^{\alpha-1}(a-1) \cdot b^{\beta-1}(b-1) c^{\gamma-1}(c-1) \dots$ ,  
или короче

$$\varphi(A) = A \frac{a-1}{a} \cdot \frac{b-1}{b} \cdot \frac{c-1}{c} \dots$$

Пример. Если  $A = 60 = 2^2 \cdot 3 \cdot 5$ , то  $\varphi(A) = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 60 = 16$ . Числа, взаимно простые с 60, суть 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

Первое решение этой проблемы содержится в работе Эйлера «*Theoremata arithmetica nova methodo demonstrata*» в «*Comm. nov. Ac. Petrop.*», VIII, p. 74. Позднее доказательство повторяется в другой работе: «*Speculationes circa quasdam insignes proprietates numerorum*», *Acta Petrop.*, VIII, p. 17.

Если же значение функции  $\varphi$  определить так, что  $\varphi(A)$  выражает количество чисел, которые взаимно просты с  $A$  и не превосходят  $A$ , то очевидно, что  $\varphi(1)$  будет уже равно не 0, а 1, а во всех остальных случаях никаких изменений от этого не произойдет. Принимая это определение, мы получаем следующую теорему.

*Если  $a, a', a'', \dots$  — всевозможные делители числа  $A$  (не исключая 1 и самого  $A$ ), то*

$$\varphi(a) + \varphi(a') + \varphi(a'') + \dots = A.$$

**Пример.** Если  $A = 30$ , то  $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$ .

**Доказательство.** Если умножить на  $A/a$  все числа, которые взаимно просты с  $a$  и не превосходят  $a$ , на  $A/a'$  — все числа, взаимно простые с  $a'$ , и т. д., то мы получим  $\varphi(a) + \varphi(a') + \varphi(a'') + \dots$  чисел, которые все не превосходят  $A$ . Но

1) все эти числа между собой различны. В самом деле, то, что все числа, которые получаются для одного и того же делителя числа  $A$ , не равны между собой, очевидно. А если бы для различных делителей  $M, N$  и соответственно взаимно простых с ними чисел  $\mu, \nu$  получались бы равные числа, т. е. если бы было  $\frac{A}{M} \mu = \frac{A}{N} \nu$ , то имело бы место  $\mu N = \nu M$ . Если предположить (что допустимо), что  $M > N$ , то  $M$ , являющееся взаимно простым с  $\mu$  и делителем числа  $\mu N$ , должно было бы также быть и делителем  $N$ , т. е. большее число было бы делителем меньшего, что невозможно;

2) среди этих чисел содержатся все числа  $1, 2, 3, \dots, A$ . Именно, если  $t$  — любое число, не превосходящее  $A$ , и  $\delta$  — наибольший общий делитель чисел  $A$  и  $t$ , то  $A/\delta$  будет делителем  $A$ , с которым  $t/\delta$  взаимно просто. Поэтому число  $t$  очевидно содержится среди тех чисел, которые получаются для делителя  $A/\delta$ ;

3) отсюда следует, что количество всех этих чисел равно  $A$ . Поэтому

$$\varphi(a) + \varphi(a') + \varphi(a'') + \dots = A.$$

## 40

Если  $\mu$  есть наибольший общий делитель чисел  $A, B, C, D, \dots$ , то можно найти числа  $a, b, c, d, \dots$  с тем свойством, что

$$aA + bB + cC + \dots = \mu.$$

**Доказательство.** Если рассматривать сначала только два числа  $A, B$ , наибольший общий делитель которых равен  $\lambda$ , то сравнение  $Ax \equiv \lambda \pmod{B}$  разрешимо (п. 30). Если его корень  $\equiv \alpha$ , то, полагая  $\frac{\lambda - A\alpha}{B} = \beta$ , получим  $\alpha A + \beta B = \lambda$ , что и требовалось.

Если присоединяется еще третье число  $C$ , и  $\lambda'$  есть наибольший общий делитель  $\lambda$  и  $C$ , то можно найти такие два числа  $k$  и  $\gamma$ , что  $k\lambda + \gamma C = \lambda'$ . Тогда  $k\alpha A + k\beta B + \gamma C = \lambda'$ . Но очевидно, что  $\lambda'$  есть общий делитель чисел  $A, B, C, \dots$ , и притом наибольший, так как если бы существовал еще больший общий делитель  $\theta$ , то выражение  $k\alpha \frac{A}{\theta} + k\beta \frac{B}{\theta} + \gamma \frac{C}{\theta} = \frac{\lambda'}{\theta}$  было бы целым числом, т. е. большее число  $\theta$  было бы делителем меньшего числа. Поэтому мы получаем требуемое, если положим  $k\alpha = a$ ,  $k\beta = b$ ,  $\gamma = c$ ,  $\lambda' = \mu$ .

Подобным же образом можно рассуждать, сколько бы новых чисел мы ни присоединяли.

Если числа  $A, B, C, D, \dots$  не имеют общих делителей, то очевидно можно добиться того, что

$$aA + bB + cC + \dots = 1.$$

## 41

Если  $p$  — простое число, и имеется  $p$  предметов, среди которых может быть любое количество одинаковых (лишь бы не все они были одинаковы), то число всех перестановок этих предметов делится на  $p$ .

**Пример.** Пять предметов  $A, A, A, B, B$  могут быть размещены десятью различными способами.

Доказательство этой теоремы легко может быть выведено из известной теории перестановок. Действительно, если среди этих предметов имеется  $a$  равных  $A$ ,  $b$  равных  $B$ ,  $c$  равных  $C$  и т. д. (где числа

$a, b, c, \dots$  могут быть равны и единице), так что

$$a + b + c + \dots = p,$$

то число перестановок равно

$$\frac{1 \cdot 2 \cdot 3 \dots p}{1 \cdot 2 \cdot 3 \dots a \cdot 1 \cdot 2 \cdot 3 \dots b \cdot 1 \cdot 2 \cdot 3 \dots c \dots}.$$

Само собой разумеется, что числитель этой дроби делится на знаменатель, так как число перестановок должно быть целым числом. Но числитель делится на  $p$ , а знаменатель, который образован из сомножителей, меньших  $p$ , на  $p$  не делится (п. 15). Поэтому число перестановок делится на  $p$  (п. 19).

Однако я надеюсь, что многим не покажется безынтересным и следующее доказательство.

Если в двух перестановках порядок предметов, из которых они образованы, отличается только тем, что тот предмет, который в одной из них занимает первое место, в другой находится на другом месте, но все предметы в обеих перестановках следуют один за другим в одном и том же порядке (считается, что за последним предметом следует первый), то мы будем называть эти перестановки подобными \*. Так, в нашем примере перестановки  $АВААВ$  и  $АВАВА$  будут подобными, так как предметы, занимающие в первой первое, второе и т. д. места, во второй в том же порядке занимают третье, четвертое и т. д. места.

Так как каждая перестановка состоит из  $p$  предметов, то для каждой, очевидно, можно найти  $p - 1$  подобных перестановок, если тот предмет, который был первым, передвигать на второе, третье и т. д. места. Если среди них нет равных, то ясно, что число всех перестановок будет делиться на  $p$ , так как оно в  $p$  раз больше, чем число всех не подобных между собой перестановок.

Предположим теперь, что две перестановки

$$PQ\dots TV\dots YZ, \quad V\dots YZPQ\dots T,$$

---

\* Если представлять себе эти перестановки записанными по кругу, так что последний предмет оказывается соседним с первым, то между подобными перестановками вообще не будет разницы, так как никакое место нельзя будет назвать ни первым, ни последним.

одна из которых получается из другой описанной передвижкой членов, равны, т. е. что  $P = V$  и т. д. Если член  $P$ , являющийся в первой перестановке первым, во второй является  $(n + 1)$ -м, то во втором ряду  $(n + 1)$ -й член будет, таким образом, равен первому,  $(n + 2)$ -й член — второму, и т. д., так что  $(2n + 1)$ -й член снова равен первому, и по той же причине и  $(3n + 1)$ -й и т. д., вообще  $(kn + m)$ -й равен  $m$ -му. (При этом, если  $kn + m > p$ , то надо либо мыслить ряд  $V...YZPQ...T$  все время снова повторяющимся сначала, либо вычитать из  $kn + m$  ближайшую меньшую кратность числа  $p$ ). Поэтому, если определить число  $k$  так, чтобы имело место  $kn \equiv 1 \pmod{p}$ , что возможно, ибо  $p$  — простое число, то мы получим, что всегда  $m$ -й член равен  $(m + 1)$ -му, т. е. каждый член равен следующему, откуда следует, что все члены равны между собой, что противоречит предположению.

## 42

Если коэффициенты  $A, B, C, \dots, N; a, b, c, \dots, n$  двух функций вида

$$(P) \quad x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \dots + N,$$

$$(Q) \quad x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \dots + N$$

все являются рациональными, но не все — целыми числами, и произведение  $(P)$  и  $(Q)$  представлено в виде

$$x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \dots + \mathfrak{Z},$$

то коэффициенты  $\mathfrak{A}, \mathfrak{B}, \dots, \mathfrak{Z}$  не могут все быть целыми.

**Доказательство.** Выразим все коэффициенты  $A, B, \dots, a, b, \dots$  в виде несократимых дробей и возьмем любое простое число  $p$ , которое входит в один или несколько из знаменателей этих дробей. Если предположить (на что мы имеем право), что  $p$  входит в знаменатель какого-нибудь дробного коэффициента у  $(P)$ , то ясно, что если  $(Q)$  разделить на  $p$ , у  $(Q)/p$  также будет хотя бы один дробный коэффициент, знаменатель которого содержит  $p$  (именно, первый коэффициент  $1/p$ ). Далее, легко видеть, что среди коэффициентов  $(P)$  имеется дробь, знаменатель которой содержит  $p$  в степени, большей, чем все предыдущие члены, и не меньшей,

чем все последующие члены. Пусть этот член есть  $Gx^s$ , а степень, в которой  $p$  входит в знаменатель дроби  $G$ , равна  $p^t$ . Подобный же член существует в  $(Q)/p$ ; пусть это  $\Gamma x^\gamma$ , и степень, в которой  $p$  входит в знаменатель дроби  $\Gamma$ , есть  $\tau$ . Очевидно, что  $t + \tau$  по меньшей мере равно 2. Тогда член  $x^{s+\gamma}$  произведения  $(P)$  и  $(Q)$  будет иметь дробный коэффициент, знаменатель которого содержит  $(t + \tau - 1)$ -ю степень числа  $p$ . Это доказывается следующим образом.

Пусть  $'Gx^{s+1}$ ,  $''Gx^{s+2}, \dots$  суть те члены, которые в  $(P)$  предшествуют члену  $Gx^s$ , а  $G'x^{s-1}$ ,  $G''x^{s-2}, \dots$  — те, которые следуют после него. Точно так же, пусть  $'\Gamma x^{\gamma+1}$ ,  $''\Gamma x^{\gamma+2}, \dots$  суть те члены, которые в  $(Q)/p$  предшествуют члену  $\Gamma x^\gamma$ , а  $\Gamma'x^{\gamma-1}$ ,  $\Gamma''x^{\gamma-2}, \dots$  — те, которые следуют после него. Тогда коэффициент члена  $x^{s+\gamma}$  в произведении  $(P)$  и  $(Q)/p$ , очевидно, равен

$$G\Gamma + 'G\Gamma' + ''G\Gamma'' + \dots + \\ + \Gamma G' + \Gamma\Gamma'' + \dots$$

Слагаемое  $G\Gamma$  есть дробь, которая после приведения к несократимому виду содержит в знаменателе  $p$  в  $(t + \tau)$ -й степени; остальные же слагаемые, если они являются дробями, содержат в знаменателе меньшие степени  $p$ , так как все они являются произведениями двух сомножителей, из которых либо знаменатель одного содержит  $p$  в степени, меньшей, чем  $\tau$ -я, а знаменатель другого — в степени, не большей, чем  $t$ -я, либо знаменатель одного содержит  $p$  в степени, меньшей, чем  $t$ -я, а знаменатель другого — в степени, не большей, чем  $\tau$ -я. Поэтому  $G\Gamma$  имеет вид  $e/fp^{t+\tau}$ , в то время как сумма остальных слагаемых имеет вид  $e'/f'p^{t+\tau-\delta}$ , где  $\delta$  есть положительное число, и  $e, f, f'$  не содержат  $p$  сомножителем. Вся сумма равна, таким образом,  $(ef' + e'fp^\delta)/ff'p^{t+\tau}$ . Так как числитель этого выражения не делится на  $p$ , то после сокращения дроби знаменатель все равно будет делиться на  $p^{t+\tau}$ . Поэтому коэффициент члена  $x^{s+\gamma}$  в произведении  $(P)$  и  $(Q)$  равен

$$\frac{ef' + e'fp^\delta}{ff'p^{t+\tau-1}},$$

т. е. является дробью, знаменатель которой содержит  $(t + \tau - 1)$ -ю степень числа  $p$ . Таким образом, теорема доказана.

Сравнение  $m$ -й степени

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Mx + N \equiv 0,$$

модулем которого является не входящее в  $A$  простое число  $p$ , не может быть разрешимо более чем  $m$  различными способами, т. е. имеет не более чем  $m$  не сравнимых по модулю  $p$  корней (см. пп. 25, 26).

Если бы это было не так, то предположим, что имеются сравнения различных степеней  $m, n, \dots$ , которые имеют более чем  $m, n, \dots$  корней, и пусть  $m$  — наименьшая такая степень, так что все подобные сравнения более низкой степени согласуются с нашей теоремой. Так как для первой степени мы эту теорему уже доказали выше (п. 26), то ясно, что  $m$  или равно 2, или больше, чем 2.

Итак, пусть сравнение

$$Ax^m + Bx^{m-1} + \dots + Mx + N \equiv 0$$

обладает по меньшей мере  $m + 1$  корнями именно  $x \equiv \alpha, x \equiv \beta, x \equiv \gamma, \dots$ , и предположим, что позволительно, что все числа  $\alpha, \beta, \gamma, \dots$  положительны и меньше, чем  $p$ , и что наименьшее из них есть  $\alpha$ . Подставим в данное сравнение  $y + \alpha$  вместо  $x$ ; пусть оно перейдет тогда в

$$A'y^m + B'y^{m-1} + C'y^{m-2} + \dots + M'y + N' \equiv 0.$$

Это сравнение, очевидно, будет удовлетворяться, если полагать  $y \equiv 0$ , или  $y \equiv \beta - \alpha$ , или  $y \equiv \gamma - \alpha$  и т. д., причем все эти корни различны между собой и число их равно  $m + 1$ . Но из того, что  $y \equiv 0$  является корнем, следует, что  $N'$  делится на  $p$ . Поэтому сравнение

$$y(A'y^{m-1} + B'y^{m-2} + \dots + M') \equiv 0 \pmod{p}$$

также удовлетворяется, если  $y$  придавать  $m$  значений  $\beta - \alpha, \gamma - \alpha, \dots$ , которые все больше 0 и меньше  $p$ , а потому при этих значениях и

$$A'y^{m-1} + B'y^{m-2} + \dots + M' \equiv 0 \text{ (п. 22),}$$

т. е. сравнение  $(m - 1)$ -й степени

$$A'y^{m-1} + B'y^{m-2} + \dots + M' \equiv 0,$$

имеет  $m$  корней, что находится в противоречии с нашей теоремой (очевидно, что  $A' = A$ , и потому  $A'$ , как и требуется, не делится на  $p$ ), хотя мы предположили, что все сравнения степени, меньшей, чем  $m$ -я, находятся с теоремой в согласии. Тем самым теорема полностью доказана.

## 44

Хотя мы предполагали, что модуль  $p$  не должен входить в коэффициент старшего члена, теорема верна не только в этом случае. Именно, если первый коэффициент, а быть может также и несколько следующих, делятся на  $p$ , то эти члены можно спокойно отбросить, и тем самым прийти к сравнению более низкой степени, у которого первый коэффициент уже не делится на  $p$ ; лишь в случае, когда все коэффициенты делятся на  $p$ , сравнение превращается в тождественное, и значение неизвестного совершенно неопределенно.

Эта теорема была впервые высказана и доказана Л а г р а н ж е м («*Mém. de l'Ac. de Berlin*», *Année 1768*, *p. 192*). Она встречается также в одной работе Л е ж а н д р а, «*Recherches d'Analyse indéterminée*», *Hist de l'Ac. de Paris*, 1785, *p. 466*. Э й л е р доказал в «*Comm. nov., Ac Petrop.*», XVIII, *p. 93*, что сравнение  $x^n - 1 \equiv 0$  не может иметь более чем  $n$  различных корней. Хотя это есть только частный случай, однако метод, которым он пользуется, легко может быть применен ко всем сравнениям. Еще более частный случай он рассматривал даже раньше, в «*Comm. nov. Ac. Petrop.*», V, *p. 6*, но использованный там метод в общем случае неприменим. Ниже, в разделе VIII, мы докажем эту теорему еще одним способом; однако, сколько бы различными на первый взгляд эти методы ни казались, все же знатоки, которые пожелают их сравнить, легко убедятся, что все они основаны на одном и том же принципе.

Так как здесь мы должны рассматривать эту теорему лишь как вспомогательную, и неуместно давать здесь ее исчерпывающее изложение, мы не будем тратить силы на то, чтобы рассматривать специально еще и составные модули.



### РАЗДЕЛ III

## О СТЕПЕННЫХ ВЫЧЕТАХ

**Вычеты членов геометрической прогрессии, начинающейся с единицы, образуют периодический ряд**

45

**Теорема.** В каждой геометрической прогрессии  $1, a, a^2, a^3, \dots$ , кроме первого члена  $1$ , имеется еще и другой член  $a^t$ , сравнимый с единицей по взаимно простому с  $a$  модулю  $p$ , с показателем  $t < p$ .

**Доказательство.** Так как модуль  $p$  взаимно прост с  $a$ , а потому и с любой степенью  $a$ , то среди членов прогрессии нет  $\equiv 0 \pmod{p}$ , и потому каждый из них сравним с одним из чисел  $1, 2, 3, \dots, (p-1)$ . Так как количество этих чисел равно  $p-1$ , то очевидно, что если взять более чем  $p-1$  членов прогрессии, их наименьшие вычеты не могут быть все различны. Поэтому среди членов  $1, a, a^2, a^3, \dots, a^{p-1}$  найдутся по крайней мере два сравнимых между собой. Пусть  $a^m \equiv a^n$  и  $m > n$ ; деля на  $a^n$  мы, получим  $a^{m-n} \equiv 1$  (п. 22), где  $m-n < p$  и  $> 0$ .

**Пример.** В прогрессии  $2, 4, 8, \dots$  первым членом, сравнимым с единицей по модулю  $13$ , оказывается  $2^{12} = 4096$ . В той же прогрессии по модулю  $23$  имеем:  $2^{11} = 2048 \equiv 1$ . Точно так же шестая степень числа  $5$ , т. е.  $15625$ , сравнима с единицей по модулю  $7$ , а пятая,  $3125$ , — по модулю  $11$ . Таким образом, в некоторых случаях уже сравнима с единицей степень с показателем, меньшим, чем  $p-1$ , в других же случаях бывает нужно доходить до  $(p-1)$ -й степени.

## 46

Если прогрессию продолжить за тот член, который сравним с единицей, то дальше будут повторяться те же самые вычеты, которые были в начале. Именно, если  $a^t \equiv 1$ , то  $a^{t+1} \equiv a$ ,  $a^{t+2} \equiv a^2$ , и т. д., до члена  $a^{2t}$ , наименьший вычет которого опять есть 1, а затем период вычетов начинается снова. Мы получаем таким образом период, содержащий  $t$  вычетов, который после того как он оканчивается, снова повторяется сначала. При этом во всей прогрессии не может встречаться других вычетов, кроме тех, которые содержатся в этом периоде. Вообще,  $a^{mt} \equiv 1$  и  $a^{mt+n} \equiv a^n$ , что в наших обозначениях мы представим так:

*Если  $r \equiv \rho \pmod{t}$ , то  $a^r \equiv a^\rho \pmod{p}$ .*

## 47

Из этой теоремы получается *простой способ отыскания вычетов степеней со сколь угодно большими показателями*, если известно, какая степень сравнима с единицей. Если, например, нужно найти остаток от деления степени  $3^{1000}$  на 13, то, так как  $3^3 \equiv 1 \pmod{13}$ , мы сначала получаем, что  $t = 3$ . Так как  $1000 \equiv 1 \pmod{3}$ , то  $3^{1000} \equiv 3 \pmod{13}$ .

## 48

Если  $a^t$  есть *наименьшая* степень, сравнимая с единицей (не считая случая  $a^0 = 1$ , который мы здесь не принимаем во внимание), то все  $t$  членов, которые образуют период вычетов, различны, что без труда можно усмотреть из доказательства в п. 45. Поэтому теорему из п. 46 можно обратить, именно: *Если  $a^m \equiv a^n \pmod{p}$ , то  $m \equiv n \pmod{t}$ .* Действительно, если бы  $m$ ,  $n$  по модулю  $t$  были не сравнимы, то их наименьшие вычеты были бы различны. Но если  $a^m \equiv a^n$ ,  $a^\nu \equiv a^n$ , то  $a^m \equiv a^\nu$ , т. е. не все степени, меньшие  $a^t$ , не сравнимы между собой, что приводит к противоречию.

Если, в частности,  $a^k \equiv 1 \pmod{p}$ , то  $k \equiv 0 \pmod{t}$ , т. е.  $k$  делится на  $t$ .

До сих пор речь шла о любых модулях, лишь бы они были взаимно просты с  $a$ . Теперь мы специально рассмотрим модули, являющиеся простыми числами, а потом на основе этого построим более общее исследование.

**Сначала рассматриваются модули,  
которые являются простыми числами**

49

**Теорема.** Если  $p$  — простое число, которое не входит в  $a$ , и  $a^t$  есть наименьшая степень  $a$ , которая сравнима с единицей по модулю  $p$ , то показатель  $t$  или равен  $p - 1$ , или является делителем этого числа.

(Ср. примеры из п. 45.)

**Доказательство.** Так как мы уже показали, что  $t$  или  $= p - 1$ , или  $< p - 1$ , нам остается только убедиться, что в последнем случае  $t$  всегда будет делителем  $p - 1$ .

I. Возьмем наименьшие положительные вычеты всех членов  $1, a, a^2, \dots, a^{t-1}$  и обозначим через  $\alpha, \alpha', \alpha'', \dots$ , так что  $\alpha \equiv 1, \alpha' \equiv a, \alpha'' \equiv a^2, \dots$ . Очевидно, что все они различны, так как если бы два члена  $a^m, a^n$  имели один и тот же вычет, то (считая, что  $m > n$ ) должно было бы быть  $a^{m-n} \equiv 1$  и  $m - n < t$ , что невозможно, потому что по условию никакая степень, меньшая, чем  $a^t$ , не сравнима с единицей. Далее, все числа  $\alpha, \alpha', \alpha'', \dots$  содержатся в ряду чисел  $1, 2, 3, \dots, p - 1$ , но не исчерпывают его целиком, так как  $t < p - 1$ . Совокупность всех чисел  $\alpha, \alpha', \alpha'', \dots$  мы обозначим через (A). Таким образом, (A) содержит  $t$  членов.

II. Выберем теперь из ряда  $1, 2, 3, \dots, p - 1$  какое-нибудь число  $\beta$ , не входящее в комплекс (A), перемножим  $\beta$  со всеми числами  $\alpha, \alpha', \alpha'', \dots$  и обозначим через  $\beta, \beta', \beta'', \dots$  наименьшие вычеты этих произведений, число которых тоже равно  $t$ . Эти вычеты должны быть все отличны как один от другого, так и от всех чисел  $\alpha, \alpha', \alpha'', \dots$ . Именно, если бы первое утверждение было неверно, то мы имели бы, например,  $\beta a^m \equiv \beta a^n$ , и потому, после деления на  $\beta$ ,  $a^m \equiv a^n$ , что противоречит доказанному выше; если же второе утверждение было бы ложным, то мы имели бы, скажем,  $\beta a^m \equiv a^n$ , откуда

(считая, что  $m < n$ )  $\beta \equiv a^n - m$ , т. е.  $\beta$  было бы сравнимо с одним из чисел  $\alpha, \alpha', \alpha'', \dots$ , что противоречит предположению. Если же  $m > n$ , то после умножения на  $a^{t-m}$  мы получим  $\beta a^t \equiv a^{t+n-m}$ , или, учитывая, что  $a^t \equiv 1$ ,  $\beta \equiv a^{t+n-m}$ , что невозможно по той же самой причине. Если совокупность всех чисел  $\beta, \beta', \beta'', \dots$ , количество которых равно  $t$ , обозначим через  $(B)$ , то в обеих совокупностях  $(A)$  и  $(B)$  будет уже  $2t$  чисел из ряда  $1, 2, 3, \dots, p-1$ . Поэтому, если  $(A)$  и  $(B)$  охватывают все эти числа, то  $t = \frac{p-1}{2}$  и теорема доказана.

III. Если же некоторые числа еще не содержатся в  $(A)$  и  $(B)$ , то пусть одно из них есть  $\gamma$ . Перемножим его со всеми числами  $\alpha, \alpha', \alpha'', \dots$ , обозначим наименьшие вычеты произведений через  $\gamma, \gamma', \gamma'', \dots$ , а совокупность всех этих вычетов — через  $(C)$ . Тогда  $(C)$  тоже будет содержать  $t$  чисел из ряда  $1, 2, 3, \dots, p-1$ , и все они будут отличны как один от другого, так и от чисел, содержащихся в  $(A)$  и  $(B)$ . Первые два утверждения доказываются так же, как в п. II, а третье следующим образом. Если бы было  $\gamma a^m \equiv \beta a^n$ , то имело бы место или  $\gamma \equiv \beta a^{n-m}$ , или  $\gamma \equiv \beta a^{t+n-m}$ , в зависимости от того,  $m < n$  или  $m > n$ ; в обоих случаях  $\gamma$  было бы таким образом, вопреки предположению, сравнимо с одним из чисел, содержащихся в комплексе  $(B)$ . Поэтому мы имеем теперь  $3t$  чисел из ряда  $1, 2, 3, \dots, p-1$ , и если других больше нет, то  $t = \frac{p-1}{3}$  и теорема доказана.

IV. Если другие числа все еще имеются, то нужно таким же способом построить четвертую совокупность чисел  $(D)$ . Так как количество чисел  $1, 2, 3, \dots, p-1$  конечно, оно рано или поздно будет исчерпано и окажется кратностью  $t$ . Таким образом,  $t$  есть делитель  $p-1$ .

### Теорема Ферма

Таким образом,  $(p-1)/t$  есть целое число, и возводя обе части сравнения  $a^t \equiv 1$  в  $\frac{p-1}{t}$ -ю степень, мы получим  $a^{p-1} \equiv 1$ , т. е.

разность  $a^p - 1$  — 1 всегда делится на  $p$ , если  $p$  — простое число, не входящее в  $a$ .

Эта теорема, которая заслуживает величайшего внимания как вследствие ее изящества, так и ввиду ее выдающейся пользы, обычно называется по имени нашедшего ее математика *теоремой Ферма* (см. «*Fermatii Opera Mathematica*», Tolosae, 1679, p. 163). Ферма не дал доказательства, но утверждал, что обладает им. Эйлер впервые опубликовал доказательство в сочинении «*Teorematum quorundam ad numeros primos spectantium demonstratio*», *Comm. Acad. Petrop.*, T. VIII\*. Оно базируется на разложении степени  $(a + 1)^p$ , из вида коэффициентов которого очень легко вывести, что  $(a + 1)^p - a^p - 1$  всегда делится на  $p$ , а потому  $(a + 1)^p - (a + 1)$  будет делиться на  $p$ , если делится  $a^p - a$ . Но так как  $1^p - 1$  всегда делится на  $p$ , то это имеет место и для  $2^p - 2$ , а потому и для  $3^p - 3$  и т. д., вообще, для  $a^p - a$ . Поэтому, если  $p$  не входит в  $a$ , то и  $a^{p-1} - 1$  будет делиться на  $p$ . Сказанного достаточно, чтобы сделать ясным сущность метода. Подобное же доказательство дал Ламберт в «*Acta Erudit.*», 1789, p. 109. Так как, однако, разложение степени бинома в значительной степени казалось чуждым теории чисел, Эйлер нашел другое доказательство, которое содержится в «*Comment. nov. Petrop.*», T. VII, p. 70 и полностью совпадает с данным нами в предыдущем пункте. В дальнейшем нам встретятся еще и другие доказательства. В этом же месте мы приведем пока еще одно, которое базируется на принципах, подобных первому доказательству Эйлера. Следующая теорема, для которой теорема Ферма является просто частным случаем, найдет ниже применение и при других исследованиях.

---

\* В более раннем сочинении он еще не достиг цели («*Comm. Acad. Petrop.*», T. VI, p. 106). В известном споре между Мопертюи и Кенигом, который возник по поводу принципа наименьшего действия, но скоро перекинулся на другие предметы, Кениг утверждал о существовании письма Лейбница, в котором содержится доказательство, полностью совпадающее с доказательством Эйлера («*Appel au public*», p. 106). Однако, даже если бы мы и не сомневались в этом свидетельстве, все же нужно отметить, что Лейбниц заведомо нигде не опубликовал своего открытия (ср. «*Hist. de l'Ac. de Berlin*», Année 1750, p. 530).

## 51

Если  $p$  — простое число, то  $p$ -я степень многочлена  $a + b + c + \dots$  сравнима по модулю  $p$  с выражением  $a^p + b^p + c^p + \dots$

**Доказательство.** Как известно,  $p$ -я степень многочлена  $a + b + c + \dots$  образуется из чисел вида  $\kappa a^\alpha b^\beta c^\gamma \dots$ , где  $\alpha + \beta + \gamma + \dots = p$ , и число  $\kappa$  указывает, сколькими способами можно переставлять  $p$  предметов, из которых  $\alpha, \beta, \gamma, \dots$  соответственно равны  $a, b, c, \dots$ . Но выше, в п. 41, мы показали, что это число всегда делится на  $p$ , если только не все предметы равны, т. е. если среди чисел  $\alpha, \beta, \gamma, \dots$  не все, кроме одного, равного  $p$ , равны 0. Отсюда следует, что у  $(a + b + c + \dots)^p$  все члены, за исключением  $a^p, b^p, c^p, \dots$ , делятся на  $p$ . Поскольку речь идет о сравнении по модулю  $p$ , их можно совсем отбросить, и тогда получится

$$(a + b + c + \dots)^p \equiv a^p + b^p + c^p + \dots$$

Если теперь все величины  $a, b, c, \dots$  равны 1, а число их равно  $k$ , то будет  $k^p \equiv k$ , как и в предыдущем пункте.

**О количестве чисел, которым соответствуют периоды,  
у которых количество членов равно  
заданному делителю числа  $p-1$**

## 52

Так как никакие числа, кроме делителей  $p-1$ , не могут быть наименьшими показателями степеней, в которые надо возводить какие-нибудь числа, чтобы сделать их сравнимыми с единицей, то возникает вопрос, все ли делители  $p-1$  здесь пригодны, и, далее, если все не делящиеся на  $p$  числа разбить на классы по показателям их наименьших сравнимых с единицей степеней, то сколько чисел будет приходиться на отдельные показатели. При этом можно сразу заметить, что достаточно рассматривать лишь все положительные числа от 1 до  $p-1$ . Действительно, очевидно, что сравнимые между собой числа нужно возводить в одну и ту же степень, чтобы сделать их сравнимыми с единицей, и потому каждое число соответ-

ствуется тому же самому показателю, что и его наименьший положительный вычет. Мы должны, таким образом, направить наше внимание на то, чтобы установить, как числа  $1, 2, 3, \dots, p-1$  разбиваются с этой точки зрения по отдельным сомножителям числа  $p-1$ . Если  $d$  — делитель  $p-1$  (к которым надо причислять также  $1$  и  $p-1$ ), то ради краткости через  $\phi(d)$  мы будем обозначать количество положительных меньших чем  $p$  чисел, для которых  $d$ -я степень есть наименьшая из всех, сравнимых с единицей.

## 53

Для того чтобы это исследование было легче понять, мы рассмотрим сначала один пример. Для  $p=19$  числа  $1, 2, 3, \dots, 18$  распределяются по делителям числа  $18$  следующим образом:

|    |                       |
|----|-----------------------|
| 1  | 1.                    |
| 2  | 18.                   |
| 3  | 7, 11.                |
| 6  | 8, 12.                |
| 9  | 4, 5, 6, 9, 16, 17.   |
| 18 | 2, 3, 10, 13, 14, 15. |

Таким образом, в этом случае  $\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(6) = 2, \phi(9) = 6, \phi(18) = 6$ . Нетрудно подметить, что каждому показателю принадлежит столько же чисел, сколько имеется чисел, которые не больше его и с ним взаимно просты, или, что, по крайней мере в этом случае, в обозначениях п. 39 имеет место  $\phi(d) = \varphi(d)$ . То, что это замечание верно всегда, мы можем доказать следующим образом.

I. Если имеется какое-нибудь число  $a$ , которое принадлежит показателю  $d$  (т. е. у которого  $d$ -я степень сравнима, а все более низкие степени не сравнимы с единицей), то все его степени  $a^2, a^3, a^4, \dots, a^d$  или их наименьшие вычеты тоже обладают первым свойством (именно, тем, что их  $d$ -е степени сравнимы с единицей), а так как это можно выразить еще и так, что наименьшие вычеты

чисел  $a, a^2, a^3, \dots, a^d$  (которые все различны между собой) являются корнями сравнения  $x^d \equiv 1$ , а это сравнение не может иметь более чем  $d$  различных корней, то ясно, что кроме наименьших вычетов чисел  $a, a^2, a^3, \dots, a^d$  между 1 и  $p-1$  включительно нет других чисел,  $d$ -я степень которых сравнима с единицей. Отсюда следует, что все принадлежащие показателю  $d$  числа содержатся среди наименьших вычетов чисел  $a, a^2, a^3, \dots, a^d$ . Каковы их значения и как велико их количество, можно определить так: если  $k$  — число, взаимно простое с  $d$ , то все степени числа  $a^k$ , показатели которых меньше, чем  $d$ , не сравнимы с единицей. Действительно, пусть  $\frac{1}{k} \equiv m (\text{mod } d)$  (см. п. 31), тогда  $a^{km} \equiv a$ ; поэтому если бы  $e$ -я степень числа  $a^k$  с  $e < d$  была сравнима с единицей, то было бы также  $a^{kme} \equiv 1$ , откуда, вопреки предположению,  $a^e \equiv 1$ . Отсюда вытекает, что наименьший вычет числа  $a^k$  принадлежит показателю  $d$ . Если же  $k$  имеет с  $d$  какой-нибудь общий делитель  $\delta$ , то наименьший вычет числа  $a^k$  не принадлежит показателю  $d$ , так как у него уже  $d/\delta$ -я степень сравнима с единицей (именно,  $kd/\delta$  будет делиться на  $d$ , т. е.  $\equiv 0 (\text{mod } d)$ , и потому  $a^{kd/\delta} \equiv 1$ ). Отсюда следует, что показателю  $d$  принадлежит столько чисел, сколько среди чисел  $1, 2, 3, \dots, d$  имеется взаимно простых с  $d$ . Однако надо иметь в виду, что этот вывод основывается на предположении, что одно число  $a$ , принадлежащее показателю  $d$ , уже имеется. Поэтому не исключена возможность, что какому-нибудь показателю вообще не принадлежит никакого числа, т. е. мы пока получили только то, что  $\phi(d)$  или  $= 0$ , или  $= \varphi(d)$ .

## 54

II. Если теперь  $d, d', d'', \dots$  суть все делители числа  $p-1$ , то так как все числа  $1, 2, 3, \dots, p-1$  распределены между этими делителями, имеет место равенство

$$\phi(d) + \phi(d') + \phi(d'') + \dots = p-1.$$

Но в п. 40 мы доказали, что

$$\varphi(d) + \varphi(d') + \varphi(d'') + \dots = p-1,$$



а из предыдущего пункта следует, что  $\psi(d)$  может быть или равно  $\varphi(d)$ , или меньше, но не больше, чем  $\varphi(d)$ , и так же обстоит дело для  $\psi(d')$  и  $\varphi(d')$  и т. д. Если какой-нибудь член (или несколько членов) ряда  $\psi(d), \psi(d'), \psi(d''), \dots$  был бы меньше, чем соответствующий член ряда  $\varphi(d), \varphi(d'), \varphi(d''), \dots$ , то сумма одного ряда не могла бы равняться сумме другого ряда. Отсюда мы, наконец, получаем, что  $\psi(d)$  *всегда равно*  $\varphi(d)$  и тем самым не зависит от величины  $p-1$ .

## 55

Наибольшее значение имеет, однако, один специальный случай предыдущей теоремы, а именно то, что *всегда существуют числа, наименьшая степень которых, сравнимая с единицей, есть  $(p-1)$ -я*, причем между 1 и  $p-1$  их столько, сколько существует чисел, не превосходящих  $p-1$  и взаимно простых с  $p-1$ . Так как доказательство этой теоремы не столь просто, как это могло бы показаться на первый взгляд, мы вследствие важности этой теоремы, дадим еще одно ее доказательство, несколько отличающееся от предыдущего, тем более, что различие методов обычно очень помогает уяснению более трудных вопросов. Разложим  $p-1$  на его простые сомножители; пусть  $p-1 = a^\alpha b^\beta c^\gamma, \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа. Тогда мы можем провести *доказательство теоремы следующим образом*.

I. Всегда можно найти число  $A$ , которое принадлежит показателю  $a^\alpha$ , и точно так же числа  $B, C, \dots$ , которые принадлежат соответственно показателям  $b^\beta, c^\gamma, \dots$ .

II. Произведение всех чисел  $A, B, C, \dots$  (или наименьший вычет этого произведения) принадлежит показателю  $p-1$ .

Это мы докажем следующим образом.

I. Если  $g$  — какое-нибудь из чисел  $1, 2, 3, \dots, p-1$ , не удовлетворяющее сравнению  $x^{(p-1)/a} \equiv 1 \pmod{p}$ , которому не могут удовлетворять все эти числа, так как его степень меньше, чем  $p-1$ , то я утверждаю, что если через  $h$  обозначить  $(p-1)/a^\alpha$ -ю степень числа  $g$ , то  $h$  или его наименьший вычет принадлежит показателю  $a^\alpha$ .

Действительно,  $a^\alpha$ -я степень числа  $h$ , очевидно, есть  $(p-1)$ -я степень числа  $g$ , т. е. сравнима с единицей, в то время как  $a^{\alpha-1}$ -я степень  $h$  есть  $(p-1)/a$ -я степень  $g$ , т. е. с единицей не сравнима;  $a^{\alpha-2}$ -я,  $a^{\alpha-3}$ -я и другие степени  $h$  подавно не могут быть сравнимы с единицей. Но показатель наименьшей сравнимой с единицей степени  $h$ , т. е. показатель, которому принадлежит  $h$ , должен (согласно п. 48) входить в число  $a^\alpha$ . Так как  $a^\alpha$  не делится ни на какие числа, кроме самого себя и более низких степеней  $a$ , отсюда необходимо вытекает, что  $a^\alpha$  должно быть показателем, которому принадлежит  $h$ . Аналогичным образом показывается, что существуют числа, которые принадлежат показателям  $b^\beta, c^\gamma, \dots$ .

II. Если мы предположим, что произведение всех чисел  $A, B, C, \dots$  принадлежит не показателю  $p-1$ , а меньшему показателю  $t$ , то  $t$  будет входить в  $p-1$  (п. 48), т. е.  $(p-1)/t$  будет целым числом, превосходящим единицу. Но легко видеть, что это частное или равно одному из простых чисел  $a, b, c, \dots$ , или по крайней мере делится на одно из них (п. 17), пусть, например, на  $a$ , так как для остальных доказательство остается тем же. Тогда  $t$  будет входить в  $(p-1)/a$ , и потому произведение  $ABC \dots$ , возведенное в  $(p-1)/a$ -ю степень, будет тоже сравнимо с единицей (п. 46). Но ясно, что отдельные числа  $B, C, \dots$  (кроме  $A$ ), возведенные в  $(p-1)/a$ -ю степень, будут сравнимы с единицей, потому что показатели  $b^\beta, c^\gamma, \dots$ , которым эти отдельные числа принадлежат, входят в  $(p-1)/a$ . Поэтому

$$A^{(p-1)/a} B^{(p-1)/a} C^{(p-1)/a} \dots \equiv A^{(p-1)/a} \equiv 1.$$

Отсюда следует, что показатель, которому принадлежит  $A$ , должен быть делителем  $(p-1)/a$  (п. 48), т. е.  $(p-1)/a^{\alpha+1}$  должно быть целым числом. Но  $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \dots}{a}$  не может быть целым (п. 15); поэтому мы должны сделать вывод, что наше предположение не может быть верным, т. е. что произведение  $ABC \dots$  действительно принадлежит показателю  $p-1$ .

Последнее доказательство выглядит несколько длиннее первого, однако, первое является менее прямым, чем второе.

## 56

Эта теорема представляет яркий пример того, какая большая осторожность часто бывает необходима в теории чисел для того, чтобы не предположить доказанным то, что в действительности еще не доказано. Л а м б е р т в уже указанной выше работе упоминает об этой теореме, но и не думает ничего говорить о необходимости ее доказательства. Никто не пытался дать доказательства, кроме Э й л е р а: «*Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*», *Comment. nov. Acad. Petrop.*, T. XVIII, 1773, p. 85 и сл. (см. в особенности параграф 37, где он подробнее распространяется о необходимости доказательства). Однако доказательство, которое дает остроумный автор, страдает двумя недостатками. Один состоит в том, что в параграфе 31 и далее автор молчаливо предполагает, что сравнение  $x^n \equiv 1$  (переводя употребляемые там способы выражения на наши обозначения) действительно имеет  $n$  различных корней, хотя до этого было доказано только, что оно может иметь не больше чем  $n$  корней; второй недостаток тот, что формула из параграфа 34 выведена только по индукции.

### Первообразные корни, основные числа, индексы

## 57

Числа, принадлежащие показателю  $p - 1$ , мы будем называть, следуя Эйлеру, первообразными корнями. Таким образом, если  $a$  — первообразный корень, то наименьшие вычеты всех степеней  $a$ ,  $a^2$ ,  $a^3, \dots, a^{p-1}$  будут различны между собой, откуда легко получается, что среди них должны находиться все числа  $1, 2, 3, \dots, p - 1$ , которых столько же, сколько и указанных наименьших вычетов, т. е. что каждое не делящееся на  $p$  число сравнимо с некоторой степенью числа  $a$ . Это замечательное свойство очень важно и может значительно облегчить арифметические операции, касающиеся сравнений, приблизительно таким же образом, как введение логарифмов облегчает операции обычной арифметики. Мы можем при желании взять какой-нибудь первообразный корень в качестве основания или основного числа и выражать через него все не делящиеся на  $p$  чис-

ла, причем, если  $a^e \equiv b \pmod{p}$ , то мы будем называть  $e$  индексом числа  $b$ . Если, например, для модуля 19 в качестве основания взят первообразный корень 2, то числам

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,  
13, 14, 15, 16, 17, 18

будут соответствовать индексы

0, 1, 13, 2, 16, 14, 6, 3, 8, 17, 12, 15,  
5, 7, 11, 4, 10, 9.

Впрочем, ясно, что если основание остается одним и тем же, то каждое число обладает многими индексами, но все они сравнимы между собой по модулю  $p - 1$ . Поэтому, когда речь будет идти об индексах, то те из них, которые сравнимы по модулю  $p - 1$ , будут рассматриваться как эквивалентные, подобно тому, как и сами числа, если они сравнимы по модулю  $p$ , считаются эквивалентными.

## Алгоритм индексов

58

Теоремы, относящиеся к индексам, совершенно эквивалентны тем, которые относятся к логарифмам.

*Индекс произведения любого числа сомножителей сравним по модулю  $p - 1$  с суммой индексов отдельных сомножителей.*

*Индекс степени какого-нибудь числа сравним по модулю  $p - 1$  с произведением индекса этого числа и показателя степени.*

Доказательства, вследствие их легкости, мы опускаем.

Отсюда видно, что если желательно построить таблицу, из которой можно было бы находить индексы всех чисел для различных модулей, то в ней можно опустить как все числа, которые больше модуля, так и все составные числа. Пример такой таблицы дан в конце этого труда (таблица 1)\*. В ней в первом вертикальном ряду

\* Таблица помещена на стр. 576.— Прим. ред.

стоят простые числа и их степени от 3 до 97, рядом с каждым из них стоят взятые за основания числа; затем идут индексы последовательных простых чисел. Точно так же, в первой строке таблицы расположены простые числа, так что можно легко и надежно найти, какой индекс соответствует заданному простому числу по заданному модулю.

Если, например,  $p = 67$  и за основание взято число 12, то индекс числа 60

$$\equiv 2 \operatorname{ind} 2 + \operatorname{ind} 3 + \operatorname{ind} 5 \equiv 58 + 9 + 39 \equiv 40 \pmod{66}.$$

### 59

*Индекс каждого значения выражения  $\frac{a}{b} \pmod{p}$  (п. 31) сравним по модулю  $p - 1$  с разностью индексов числителя  $a$  и знаменателя  $b$ , если только числа  $a$  и  $b$  не делятся на  $p$ .*

Именно, если  $c$  — какое-нибудь значение этого выражения, то  $bc \equiv a \pmod{p}$ , и потому

$$\operatorname{ind} b + \operatorname{ind} c \equiv \operatorname{ind} a \pmod{p - 1},$$

откуда

$$\operatorname{ind} c \equiv \operatorname{ind} a - \operatorname{ind} b.$$

Таким образом, если имеется таблица, из которой можно находить индекс, соответствующий любому числу по любому простому модулю, и другая таблица, из которой можно получить число, принадлежащее заданному индексу, то можно очень легко решать все сравнения первой степени, так как все они сводятся к таким, у которых модуль есть простое число (п. 30). Если, например, дано сравнение  $29x + 7 \equiv 0 \pmod{47}$ , то  $x \equiv \frac{-7}{29} \pmod{47}$ , и потому  $\operatorname{ind} x \equiv \operatorname{ind} (-7) - \operatorname{ind} (29) \equiv \operatorname{ind} 40 - \operatorname{ind} 29 \equiv 15 - 43 \equiv 18 \pmod{46}$ .

Но индекс 18 принадлежит числу 3. Поэтому  $x \equiv 3 \pmod{47}$ .

Впрочем, вторую таблицу мы не приложили. Вместо нее нам может служить другая таблица, как мы покажем в разделе VI.

О корнях сравнения  $x^n \equiv A$ 

60

Аналогично тому, как в п. 31 мы обозначали корни сравнений первой степени, мы в дальнейшем будем употреблять специальное обозначение и для корней чистых сравнений более высокой степени. Именно, подобно тому, как  $\sqrt[n]{A}$  обозначает не что иное как корень уравнения  $x^n = A$ , так и любой корень сравнения  $x^n \equiv A \pmod{p}$  будет обозначаться так же, но с добавлением модуля:  $\sqrt[n]{A} \pmod{p}$ . Мы будем говорить, что это выражение  $\sqrt[n]{A} \pmod{p}$  обладает столькими значениями, сколько оно имеет значений, не сравнимых по модулю  $p$ , так как все сравнимые по  $p$  значения следует рассматривать как эквивалентные (п. 26). Кроме того, ясно, что если  $A$  и  $B$  сравнимы по модулю  $p$ , то выражения  $\sqrt[n]{A} \pmod{p}$  и  $\sqrt[n]{B} \pmod{p}$  будут между собой эквивалентны.

Если положить  $\sqrt[n]{A} \equiv x \pmod{p}$ , то  $n \operatorname{ind} x \equiv \operatorname{ind} A \pmod{p-1}$ . Из этого сравнения по правилам предыдущего раздела получаются значения  $\operatorname{ind} x$ , а из них, — соответствующие значения  $x$ . Легко видеть, что  $x$  обладает столькими же значениями, сколько корней имеет сравнение  $n \operatorname{ind} x \equiv \operatorname{ind} A \pmod{p-1}$ . Таким образом,  $\sqrt[n]{A}$  имеет только одно значение, если  $n$  взаимно просто с  $p-1$ ; если же числа  $n$  и  $p-1$  имеют наибольший общий делитель  $\delta$ , то  $\operatorname{ind} x$  имеет  $\delta$  значений, не сравнимых по модулю  $p-1$ , а потому и  $\sqrt[n]{A}$  имеет столько же значений, не сравнимых по модулю  $p$ , если только  $\operatorname{ind} A$  делится на  $\delta$ . Если же это условие не выполнено, то  $\sqrt[n]{A}$  не будет иметь вещественных значений.

**Пример.** Пусть нужно найти значения выражения  $\sqrt[15]{11} \pmod{19}$ . Для этого нужно решить сравнение  $15 \operatorname{ind} x \equiv \operatorname{ind} 11 \equiv 6 \pmod{18}$ , откуда находятся три значения  $\operatorname{ind} x \equiv 4, 10, 16 \pmod{18}$ . Им соответствуют значения  $x \equiv 6, 9, 4 \pmod{19}$ .

Как ни прост этот метод, когда под рукой есть нужные таблицы, все же не следует забывать, что он является косвенным. Поэтому имеет смысл потратить усилия на то, чтобы исследовать, насколько сильны прямые методы, причем мы приведем здесь то, что может быть выведено из предыдущего, остальное же, что требует более глубоких рассмотрений, оставим до раздела VIII.

Начнем с простейшего случая, когда  $A = 1$ , т. е. когда ищутся корни сравнения  $x^n \equiv 1 \pmod{p}$ . Таким образом, если за основание взять произвольный первообразный корень, то здесь должно быть  $n \operatorname{ind} x \equiv 0 \pmod{p-1}$ . Если  $n$  взаимно просто с  $p-1$ , то это сравнение будет иметь один единственный корень, именно,  $\operatorname{ind} x \equiv 0 \pmod{p-1}$ , и потому в этом случае  $\sqrt[n]{1} \pmod{p}$  имеет единственное значение, именно,  $\equiv 1$ . Если же числа  $n$  и  $p-1$  имеют (наибольший) общий делитель  $\delta$ , то полным решением сравнения  $n \operatorname{ind} x \equiv 0 \pmod{p-1}$  будет  $\operatorname{ind} x \equiv 0 \pmod{\frac{p-1}{\delta}}$  (п. 29), т. е.  $\operatorname{ind} x$  должен будет быть сравнимым по модулю  $p-1$  с каким-нибудь из чисел

$$0, \quad \frac{p-1}{\delta}, \quad \frac{2(p-1)}{\delta}, \quad \frac{3(p-1)}{\delta}, \dots, \frac{(\delta-1)(p-1)}{\delta},$$

или, другими словами, обладать  $\delta$  значениями, не сравнимыми по модулю  $p-1$ ; поэтому в этом случае  $x$  также имеет  $\delta$  различных (несравнимых по модулю  $p$ ) значений. Отсюда явствует, что

выражение  $\sqrt[\delta]{1}$  тоже имеет  $\delta$  различных значений, индексы которых в точности совпадают с указанными перед этим числами.

Поэтому выражение  $\sqrt[\delta]{1} \pmod{p}$  совершенно эквивалентно выражению  $\sqrt[n]{1} \pmod{p}$ , т. е. сравнение  $x^\delta \equiv 1 \pmod{p}$  имеет те же корни, что и  $x^n \equiv 1 \pmod{p}$ . Однако первое имеет более низкую степень, чем второе, если только  $\delta$  и  $n$  не равны между собой.

**Пример.**  $\sqrt[15]{1} \pmod{19}$  имеет три значения, потому что 3 есть наибольший общий делитель чисел 15 и 18, и эти значения одновременно являются значениями  $\sqrt[3]{1} \pmod{19}$ . Последние же суть 1, 7, 11.

## 62

Итак, благодаря этой редукции мы получаем то преимущество, что нам не надо решать никаких других сравнений вида  $x^n \equiv 1$ , кроме тех, у которых  $n$  является делителем  $p-1$ . Ниже мы покажем, что сравнения этого вида всегда могут быть еще упрощены, однако пока изложенного материала для этого недостаточно. Сейчас мы можем закончить только один случай, именно, тот, когда  $n=2$ . В самом деле, очевидно, что  $+1$  и  $-1$  дают все значения выражения  $\sqrt{1}$ , так как больше двух значений оно иметь не может, а  $+1$  и  $-1$  всегда несравнимы между собой, кроме случая, когда модуль равен 2; в этом случае непосредственно ясно, что  $\sqrt[n]{1}$  может иметь только одно значение. Из этого следует, что  $+1$  и  $-1$  будут также значениями выражения  $\sqrt[2m]{1}$ , в случае, когда  $m$  взаимно просто с  $(p-1)/2$ . Это всегда имеет место, если модуль таков, что  $(p-1)/2$  является простым числом (если при этом в точности  $p-1=2m$ , то все числа 1, 2, 3, ...,  $p-1$  являются корнями), например, если  $p=3, 5, 7, 11, 23, 47, 59, 83, 107, \dots$ . В качестве следствия здесь можно было бы добавить, что индекс числа  $-1$  всегда  $\equiv \frac{p-1}{2} \pmod{p-1}$ , какой бы первообразный корень мы ни взяли. Действительно,  $2 \operatorname{ind}(-1) \equiv 0 \pmod{p-1}$ ; поэтому  $\operatorname{ind}(-1)$  или  $\equiv 0$ , или  $\equiv \frac{p-1}{2} \pmod{p-1}$ . Но 0 всегда является индексом числа  $+1$ , а  $+1$  и  $-1$  всегда должны иметь различные индексы (кроме случая  $p=2$ , который мы здесь исключаем).

## 63

В п. 60 мы показали, что выражение  $\sqrt[n]{A} \pmod{p}$  имеет или  $\delta$  различных значений, где  $\delta$  есть наибольший общий делитель



чисел  $n$  и  $p - 1$ , или ни одного значения. Подобно тому, как выше мы доказали, что  $\sqrt[n]{A}$  и  $\sqrt[\delta]{A}$  эквиваленты, если  $A \equiv 1$ , так сейчас мы докажем более общий факт, что выражение  $\sqrt[n]{A}$  всегда может быть сведено к выражению вида  $\sqrt[\delta]{B}$ , с которым оно эквивалентно. Именно, обозначим какое-нибудь значение нашего выражения через  $x$ , так что  $x^n \equiv A$ . Если теперь  $t$  — какое-нибудь значение выражения  $\frac{\delta}{n} \pmod{p-1}$ , которое, как явствует из п. 31, обладает вещественными значениями, то  $x^{nt} \equiv A^t$ . Но  $x^{nt} \equiv x^\delta$  вследствие того, что  $tn \equiv \delta \pmod{p-1}$ . Отсюда  $x^\delta \equiv A^t$ , и потому любое значение  $\sqrt[n]{A}$  будет также значением  $\sqrt[\delta]{A^t}$ . Таким образом, если выражение  $\sqrt[n]{A}$  имеет вещественные значения, то оно совершенно эквивалентно выражению  $\sqrt[\delta]{A^t}$ , ибо последнее не имеет других значений и имеет все значения первого, хотя может случиться, что если  $\sqrt[n]{A}$  не имеет вещественных значений,  $\sqrt[\delta]{A^t}$  все же ими обладает.

**Пример.** Если отыскиваются значения выражения  $\sqrt[21]{2} \pmod{31}$ , то наибольший общий делитель чисел 21 и 30 равен 3, и одно из значений выражения  $\frac{3}{21} \pmod{30}$  тоже равно 3. Поэтому, если выражение  $\sqrt[21]{2}$  обладает вещественными значениями, то оно будет эквивалентно выражению  $\sqrt[3]{2^3}$  или  $\sqrt[3]{8}$ , и действительно, оказывается, что значения второго выражения, именно 2, 10, 19, удовлетворяют также и первому.

Для того чтобы избежать опасности, что мы будем применять эту операцию понапрасну, мы должны получить *правило, при помощи которого можно сразу узнавать, допускает  $\sqrt[n]{A}$  вещественные*

значения или нет. Если имеется таблица индексов, то вопрос ясен; действительно, из п. 60 вытекает, что вещественные значения существуют или нет в зависимости от того, делится или нет на  $\delta$  индекс числа  $A$  относительно какого-нибудь взятого за основание первообразного корня. Однако это можно узнать и без помощи такой таблицы. Именно, если индекс числа  $A$  равен  $k$ , то если он делится на  $\delta$ ,  $k(p-1)/\delta$  будет делиться на  $p-1$ , и обратно. Далее, индекс числа  $A^{(p-1)/\delta}$  равен  $k(p-1)/\delta$ . Поэтому, если  $\sqrt[n]{A} \pmod{p}$  имеет вещественные значения, то  $A^{(p-1)/\delta}$  будет сравнимо с единицей, в противном же случае — нет. Так, в примере предыдущего пункта  $2^{10} = 1024 \equiv 1 \pmod{31}$ , откуда следует, что  $\sqrt[21]{2} \pmod{31}$  имеет вещественные значения. Таким же образом мы убеждаемся отсюда, что  $\sqrt{-1} \pmod{p}$  всегда имеет два вещественных значения, если  $p$  имеет вид  $4m+1$ , и ни одного значения, если  $p$  имеет вид  $4m+3$ , потому что  $(-1)^{2m} = 1$  и  $(-1)^{2m+1} = -1$ . Эта изящная теорема, которая обычно высказывается в следующей форме: если  $p$  — простое число вида  $4m+1$ , то всегда можно найти квадрат целого числа  $a^2$  с тем свойством, что  $a^2+1$  будет делиться на  $p$ ; если же  $p$  — простое число вида  $4m-1$ , то такого квадрата не существует, — была таким же способом доказана Эйлером, в «*Comm. nov. Acad. Petrop.*», Т. XVIII, 1773, р. 112. Другое доказательство он дал еще намного раньше, в «*Comm. nov.*», Т. V, р. 5, вышедшем в 1760 г. В более раннем сочинении, в «*Comm. nov.*», Т. IV, р. 25, он еще не пришел к доказательству. Позднее также и Лагранж дал в «*Nouveaux Mém. de l'Ac. de Berlin*», А. 1775, р. 342, новое доказательство теоремы. Еще одно доказательство мы дадим в следующем разделе, который будет специально посвящен этому предмету.

После того, как мы научились все выражения  $\sqrt[n]{A} \pmod{p}$  сводить к таким, у которых  $n$  есть делитель числа  $p-1$ , и одновременно получили критерий для того, чтобы узнавать, обладают они

вещественными значениями или нет, мы рассмотрим теперь такие выражения  $\sqrt[n]{A} \pmod{p}$ , у которых  $n$  есть делитель  $p-1$ , несколько подробнее. Сначала мы покажем, в какой связи находятся между собой отдельные значения выражения, а затем укажем некоторые специальные приемы, при помощи которых очень часто можно найти одно значение выражения.

*Во-первых*, если  $A \equiv 1$  и  $r$  — какое-нибудь одно из значений выражения  $\sqrt[n]{1} \pmod{p}$ , т. е.  $r^n \equiv 1 \pmod{p}$ , то и все степени  $r$  будут значениями этого выражения; а среди них различных между собой будет столько, сколько единиц содержит показатель, которому принадлежит  $r$  (п. 48). Поэтому, если  $r$  есть значение, принадлежащее показателю  $n$ , то степени  $r, r^2, r^3, \dots, r^n$  (где вместо последней можно также взять единицу) будут охватывать все значения выражения  $\sqrt[n]{1} \pmod{p}$ . Вопрос же о том, какие существуют вспомогательные средства для отыскания таких значений, которые принадлежат показателю  $n$ , мы более подробно рассмотрим в разделе VIII.

*Во-вторых*, если  $A$  несравнимо с единицей, и одно значение выражения  $\sqrt[n]{A} \pmod{p}$ , которое мы обозначим через  $z$ , известно, то остальные значения можно искать следующим образом. Если (как мы показали выше)

$$1, r, r^2, \dots, r^{n-1}$$

суть все значения выражения  $\sqrt[n]{1}$ , то

$$z, zr, zr^2, \dots, zr^{n-1}$$

будут всеми значениями выражения  $\sqrt[n]{A}$ . Действительно, то, что все эти значения удовлетворяют сравнению  $x^n \equiv A$ , вытекает из того, что если взять какое-нибудь из них, скажем  $\equiv zr^k$ , то его  $n$ -я степень, именно  $z^n r^{nk}$ , вследствие того, что  $r^n \equiv 1$  и  $z^n \equiv A$ , будет сравнима с  $A$ , а то, что все эти значения различны, легко следует из п. 23. Других же значений, кроме этих, число которых рав-

но  $n$ , выражение  $\sqrt[n]{A}$  иметь не может. Так, например, если одно из значений выражения  $\sqrt[n]{A}$  равно  $z$ , то другое будет равно  $-z$ . Наконец, мы должны сделать вывод, что все значения выражения  $\sqrt[n]{A}$  найти нельзя, если одновременно не известны все значения выражения  $\sqrt[n]{1}$ .

## 66

Вторая задача, которую мы себе поставили, заключалась в том, чтобы показать, в каком случае может быть непосредственно найдено одно значение выражения  $\sqrt[n]{A} \pmod{p}$  (где  $n$  предполагается делителем  $p-1$ ). Это тот случай, когда какое-нибудь значение сравнимо с какой-нибудь степенью  $A$ , и так как этот случай встречается нередко, будет не лишним немного на нем задержаться. Пусть одно из таких значений, если они вообще существуют, есть  $z$ , так что  $z \equiv A^k$  и  $A \equiv z^n \pmod{p}$ . Отсюда следует  $A \equiv A^{kn}$ . Поэтому, если имеется число  $k$  с тем свойством, что  $A \equiv A^{kn}$ , то  $A^k$  будет искомым значением. А это условие эквивалентно тому, что  $1 \equiv kn \pmod{t}$ , где  $t$  обозначает показатель, которому принадлежит  $A$  (пп. 46, 48). Для того, чтобы это сравнение было возможно, необходимо, чтобы  $n$  было взаимно просто с  $t$ . В этом случае  $k \equiv \frac{1}{n} \pmod{t}$ ; если же  $t$  и  $n$  имеют общий делитель, то ни одно значение  $z$  не может быть сравнимо со степенью числа  $A$ .

## 67

Так как, однако, для такого решения нужно знать само  $t$ , мы посмотрим, как можно поступать, когда это число не известно. Прежде всего, очевидно, что  $t$  должно входить в  $(p-1)/n$ , если только  $\sqrt[n]{A} \pmod{p}$  имеет вещественные значения, что мы здесь все время предполагаем. Действительно, если какое-нибудь значение этого выражения равно  $y$ , то как  $y^{p-1} \equiv 1$ , так и  $y^n \equiv A \pmod{p}$ . Если

возвести обе части последнего сравнения в  $(p-1)/n$ -ю степень, то получится  $A^{(p-1)/n} \equiv 1$ , и потому  $(p-1)/n$  должно делиться на  $t$  (п. 48). Если теперь  $(p-1)/n$  взаимно просто с  $n$ , то сравнение из предыдущего пункта, а именно,  $kn \equiv 1$ , разрешимо также и по модулю  $(p-1)/n$ , и удовлетворяющее сравнению по этому модулю значение  $k$  будет, очевидно, удовлетворять тому же сравнению и по модулю  $t$ , который входит в  $(p-1)/n$  (п. 5). В этом случае цель достигнута. Если же  $(p-1)/n$  не взаимно просто с  $n$ , то выбросим из  $(p-1)/n$  все простые сомножители, которые одновременно входят в  $n$ . Тогда мы получим взаимно простое с  $n$  число  $(p-1)/nq$ , где  $q$  обозначает произведение всех тех простых сомножителей, которые мы выбросили. Если теперь условие, к которому мы пришли в предыдущем пункте, а именно, что  $t$  взаимно просто с  $n$ , выполняется, то  $t$  будет также взаимно просто с  $q$  и потому будет входить и в  $(p-1)/nq$ . Поэтому, если решить сравнение  $kn \equiv 1 \pmod{\frac{p-1}{nq}}$  (что возможно, так как  $n$  взаимно просто с  $(p-1)/nq$ ), то значение  $k$  будет удовлетворять также и сравнению по модулю  $t$ , что и требовалось. В целом этот прием состоит в том, чтобы найти число, которым можно заменить неизвестное нам число  $t$ . Однако нужно иметь в виду, что в случае, когда  $(p-1)/n$  не взаимно просто с  $n$ , мы предполагали, что выполнено условие из предыдущего пункта. Если же это условие не выполнено, то все выводы теряют силу; и если при невнимательном следовании указанным правилам мы найдем значение  $z$ ,  $n$ -я степень которого несравнима с числом  $A$ , то это будет указывать на то, что условие не выполнено и потому этот метод вообще нельзя применять.

Однако и в этом случае потраченные усилия часто бывают полезны, и имеет смысл исследовать, как это неверное значение относится к правильному. Предположим, что  $k, z$  определены согласно правилам, но что  $z^n$  не сравнимо с  $A$  по модулю  $p$ . Если только мы можем определить значения выражения  $\sqrt[n]{A/z^n} \pmod{p}$ , то умножая каждое из них на  $z$ , мы получим значения  $\sqrt[n]{A}$ . Действи-

тельно, если  $v$  — какое-нибудь значение  $\sqrt[n]{A/z^n}$ , то  $(vz)^n \equiv A$ . Но выражение  $\sqrt[n]{A/z^n}$  проще, чем  $\sqrt[n]{A}$ , постольку поскольку  $\frac{A}{z^n} \pmod{p}$  по большей части принадлежит меньшему показателю, чем  $A$ . Именно, если  $d$  есть наибольший общий делитель  $t$  и  $q$ , от  $\frac{A}{z^n} \pmod{p}$  будет принадлежать показателю  $d$ , что доказывается следующим образом. Если вместо  $z$  подставить его значение, мы получим  $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \pmod{p}$ . Но  $kn-1$  делится на  $(p-1)/nq$  (согласно предыдущему пункту), а  $(p-1)/n$  — на  $t$  (там же), откуда  $(p-1)/nd$  делится на  $t/d$ . Далее,  $t/d$  взаимно просто с  $q/d$  (по условию), и потому также  $(p-1)/nd$  делится на  $tq/d^2$ , или  $(p-1)/nq$  — на  $t/d$ , и, таким образом,  $kn-1$  делится на  $t/d$  и  $(kn-1)d$  — на  $t$ . Из этого следует, что  $A^{(kn-1)d} \equiv 1 \pmod{p}$ , откуда легко вывести, что  $A/z^n$ , возведенное в  $d$ -ю степень, сравнимо с единицей. А то, что  $A/z^n$  не может принадлежать показателю, меньшему, чем  $d$ , хотя и может быть легко доказано, но мы на этом останавливаться не будем, так как для нашей цели это не требуется. Таким образом, мы заведомо установили, что  $A/z^n \pmod{p}$  всегда принадлежит меньшему показателю, чем  $A$ , за исключением того единственного случая, когда  $t$  входит в  $q$ , и потому  $d = t$ .

Однако, какая польза в том, что  $A/z^n$  принадлежит меньшему показателю, чем  $A$ ? Чисел, которые могут выступать в роли  $A$ , больше, чем чисел, которые могут выступать в роли  $A/z^n$ , и если мы должны получить выражения вида  $\sqrt[n]{A}$  по одному и тому же модулю, то теперь мы имеем то преимущество, что многие из них можно вывести из одного и того же источника.

Так, например, мы всегда будем в состоянии определить хотя бы одно значение выражения  $\sqrt[n]{A} \pmod{29}$ , если только известны значения  $\sqrt[n]{-1} \pmod{29}$  (которые суть  $\pm 12$ ). Действительно, из предыдущего пункта явствует, что значение подобного выражения всегда можно найти непосредственно, если  $t$  нечетно, и что  $d = 2$ ,

если  $t$  четно; но показателю 2 не принадлежат никакие числа, кроме  $-1$ .

**Примеры.** Найдем значения  $\sqrt[3]{31} \pmod{37}$ . Здесь  $p-1 = 36$ ,  $n=3$ ,  $\frac{p-1}{3} = 12$ , и потому  $q = 3$ . Поэтому должно быть  $3k \equiv 1 \pmod{4}$ , и это имеет место, если положить  $k = 3$ . Отсюда  $z \equiv 31^3 \equiv 6 \pmod{37}$ , и, действительно, мы находим, что  $6^3 \equiv 31 \pmod{37}$ . Если значения выражения  $\sqrt[3]{1} \pmod{37}$  известны, то и остальные значения  $\sqrt[3]{6}$  могут быть определены. Но значения  $\sqrt[3]{1}$  суть 1, 10, 26, и, умножая их на 6, мы и получим остальные значения  $\equiv 23$  и 8.

Если же отыскивается значение выражения  $\sqrt[3]{3} \pmod{37}$ , то здесь  $n=2$ ,  $\frac{p-1}{n} = 18$ , и потому  $q = 2$ . Поэтому должно быть  $2k \equiv 1 \pmod{9}$ , откуда  $k \equiv 5 \pmod{9}$ . Следовательно,  $z \equiv 3^5 \equiv 21 \pmod{37}$ . Но  $21^2$  не сравнимо с 3, а сравнимо с 34. Однако  $\frac{3}{34} \equiv -1 \pmod{37}$  и  $\sqrt{-1} \equiv \pm 6 \pmod{37}$ . Отсюда получаются верные значения  $\pm 6 \cdot 21 \equiv \pm 15$ .

Вот примерно то, что мы можем здесь сообщить относительно отыскания таких выражений. Известно, что прямые методы часто оказываются довольно длинными, однако этот недостаток присущ не всем прямым методам теории чисел, и потому мы не могли удержаться от того, чтобы не показать, как много они могут здесь дать. Следует также заметить и то, что в нашу задачу не входит подробнее развивать специальные приемы, которые нередко может найти опытный вычислитель.

### Связь между индексами в различных системах

Мы возвращаемся теперь к корням, которые называли первообразными. Мы покажем, что если за основание взят любой первообразный корень, то все числа, индексы которых взаимно просты с  $p-1$ , также являются первообразными корнями, и что, кроме

них, других первообразных корней нет, так что тем самым одновременно становится известным количество всех первообразных корней (см. п. 53). Какой первообразный корень мы берем за основание, вообще говоря, зависит от нашего желания, откуда видно, что здесь, как и в логарифмическом исчислении, возможны различные системы\*; мы рассмотрим, каким образом они между собой связаны. Пусть  $a$  и  $b$  — два первообразных корня, и  $m$  — какое-нибудь другое число, и пусть, если за основание взято  $a$ , то у числа  $b$  индекс  $\equiv \beta$ , а у числа  $m$  индекс  $\equiv \mu \pmod{p-1}$ ; если же за основание взято  $b$ , то пусть у  $a$  индекс  $\equiv \alpha$ , а у  $m$  индекс  $\equiv \nu \pmod{p-1}$ . Тогда  $\alpha\beta \equiv 1 \pmod{p-1}$ . Действительно, по предположению,  $a^\beta \equiv b$ , и потому  $a^{\alpha\beta} \equiv b^\alpha \equiv a \pmod{p}$ , откуда  $\alpha\beta \equiv 1 \pmod{p-1}$ . Аналогичным рассуждением находим, что  $\nu \equiv \alpha\mu$  и  $\mu \equiv \beta\nu \pmod{p-1}$ . Поэтому, если имеется таблица индексов, составленная для основания  $a$ , она легко может быть превращена в другую, основанием которой есть  $b$ . Действительно, если для основания  $a$  индекс числа  $b$  сравним с  $\beta$ , то для основания  $b$  индекс числа  $a$  сравним с  $\frac{1}{\beta} \pmod{p-1}$ , и если на это число умножить все индексы таблицы, то мы получим все индексы для основания  $b$ .

## 70

Хотя заданное число может получать различные индексы, если за основание брать все новые и новые первообразные корни, у этих индексов все же будет то общее, что все они имеют с  $p-1$  один и тот же наибольший общий делитель. Действительно, если индекс заданного числа для основания  $a$  есть  $m$ , а для основания  $b$  есть  $n$ , и мы предположим, что наибольшие общие делители  $\mu, \nu$  этих индексов с  $p-1$  не равны между собой, то один из них будет больше другого, например,  $\mu > \nu$ , и потому  $\mu$  не будет входить в  $\nu$ . Но если обозначить через  $\alpha$  индекс числа  $a$ , когда за основание взято  $b$ , то, согласно предыдущему пункту,  $n \equiv \alpha m \pmod{p-1}$ ,

---

\* Разница состоит только в том, что в случае логарифмов количество возможных систем бесконечно велико, в нашем же случае оно лишь равно числу первообразных корней. В самом деле, сравнимые между собой основания, очевидно, порождают одинаковые системы.



и потому  $\mu$  также будет входить в  $n$ , что противоречит нашему предположению.

То, что этот наибольший общий делитель индекса заданного числа и числа  $p-1$  не зависит от основания, вытекает также и из того, что он равен  $(p-1)/t$ , где  $t$  обозначает показатель, которому принадлежит число, об индексе которого идет речь. Действительно, если индекс для некоторого произвольного основания равен  $k$ , то  $t$  есть наименьшее число (не считая нуля) такого рода, что произведение  $k$  и  $t$  будет кратностью  $p-1$  (ср. пп. 48 и 58), т. е. есть наименьшее, за исключением нуля, значение выражения  $\frac{0}{k} \pmod{p-1}$ ; а то, что оно равно наибольшему общему делителю чисел  $k$  и  $p-1$ , без труда вытекает из п. 28.

## 71

Далее, легко доказать, что основание всегда можно выбрать так, что принадлежащее показателю  $t$  число получит любое заданное значение индекса, лишь бы его наибольший общий делитель с  $p-1$  был равен  $(p-1)/t$ . Если этот наибольший общий делитель мы для краткости обозначим через  $d$ , если, далее, заданный индекс  $\equiv dm$ , а индекс заданного числа, когда за основание взят какой-то первообразный корень  $a$ ,  $\equiv dn$ , то  $m$  и  $n$  будут взаимно просты с  $\frac{p-1}{a}$  и с  $t$ . Если тогда  $\varepsilon$  есть значение выражения  $\frac{dm}{dn} \pmod{p-1}$ , которое взаимно просто с  $p-1$ , то  $a^\varepsilon$  будет первообразным корнем, и если его взять за основание, то заданное число получит требуемый индекс  $dm$  (действительно,  $a^{\varepsilon dm} \equiv a^{dn} \equiv$  с заданным числом). А то, что выражение  $\frac{dn}{dm} \pmod{p-1}$  обладает значением, взаимно простым с  $p-1$ , может быть доказано следующим образом. Согласно пп. 31, 32 это выражение эквивалентно следующему:  $\frac{n}{m} \left( \pmod{\frac{p-1}{d}} \right)$  или  $\frac{n}{m} \pmod{t}$ , — а все значения этого последнего взаимно просты с  $t$ ; действительно, если бы какое-нибудь значение  $e$  имело с  $t$  общий делитель, то этот делитель должен был бы входить и в  $me$ , а потому также и в число  $n$ , которое сравнимо с  $me$  по модулю  $t$ . Но это противоречит предпо-

ложению, что  $m$  взаимно просто с  $t$ . Таким образом, если все простые делители числа  $p-1$  входят также и в  $t$ , то все значения выражения  $\frac{n}{m} \pmod{t}$  будут взаимно просты с  $p-1$  и число их будет равно  $d$ . Если же  $p-1$  содержит еще и другие простые делители  $f, g, h, \dots$ , которые в  $t$  не входят, то пусть  $\frac{n}{m} \pmod{t} \equiv e$  — какое-нибудь значение выражения  $\frac{n}{m} \pmod{t}$ . Тогда, так как числа  $t, f, g, h, \dots$  попарно взаимно просты, можно найти такое число  $\varepsilon$ , которое по модулю  $t$  сравнимо с числом  $e$ , а по модулям  $f, g, h, \dots$  — с любыми взаимно простыми с этими модулями числами (п. 32). Такое число не будет тогда делиться ни на один простой сомножитель числа  $p-1$ , т. е. будет взаимно просто с  $p-1$ , что и требовалось. Наконец, из комбинаторных соображений без труда получается, что число таких значений равно  $\frac{p-1}{p} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h} \dots$ . Однако, чтобы этот экскурс не слишком затянулся, мы доказательство опустим, ибо для нашей цели оно не является столь уж необходимым.

## Основные числа, служащие специальным целям

### 72

Хотя, вообще говоря, совершенно безразлично, какой первообразный корень берется за основание, все же иногда *одни основные числа могут иметь преимущества перед другими*. В таблице 1 мы всегда брали за основание число 10, если только оно было первообразным корнем; в остальных случаях мы всегда определяли основание так, чтобы индекс числа 10 был наименьшим из возможных, т. е. чтобы он был равен  $(p-1)/t$ , где  $t$  обозначает показатель, которому принадлежит 10. Какое преимущество мы благодаря этому имеем, мы покажем в разделе VI, где эта таблица будет снова использована для другой цели. Так как, однако, и здесь еще может остаться некоторый произвол, то мы, для определенности, из всех удовлетворяющих указанному выше условию первообразных корней всегда выбирали за основание наименьший.

Так, например, для  $p = 73$ , когда  $t = 8$  и  $d = 9$ ,  $a^\varepsilon$  имеет  $\frac{72 \cdot 2}{8 \cdot 3} = 6$  значений, а именно, значения 5, 14, 20, 28, 39, 40. Мы взяли за основание наименьшее из них — число 5.

## Метод отыскания первообразных корней

### 73

*Методы отыскания первообразных корней большей частью сводятся к пробам.* Если то, что мы изложили в п. 55, сопоставить с тем, что будет сказано ниже относительно решения сравнения  $x^n \equiv 1$ , то это и будет почти все, что можно получить прямыми методами. Э й л е р в «*Opusc. Analyt.*», Т. I, р. 152, признает, что ему представляется исключительно трудным находить такие числа, и что их истинная сущность должна быть причислена к наиболее глубоким секретам чисел. Однако посредством проб они довольно легко определяются следующим образом. (Имеющий навык будет знать, что продолжительность выкладок может быть сокращена многочисленными специальными приемами; однако научиться этому можно гораздо быстрее на практике, чем следуя теоретическим предписаниям.)

1. Берем любое взаимно простое с  $p$  (так все время будет обозначаться модуль) число  $a$  (в большинстве случаев ради сокращения вычислений хорошо брать его по возможности маленьким, например, брать число 2) и определяем его период (п. 46), для чего находим наименьшие вычеты его степеней, до тех пор, пока не дойдем до некоторой степени  $a^t$ , наименьший вычет которой равен 1\*. Если  $t = p - 1$ , то  $a$  есть первообразный корень.

2. Если же  $t < p - 1$ , то берем другое число  $b$ , которое не содержится в периоде числа  $a$ , и ищем подобным же образом его период. Если показатель, которому принадлежит  $b$ , обозначить через  $u$ , то легко убедиться, что  $u$  не может быть ни равным  $t$ , ни делителем  $t$ ; действительно, в обоих случаях было бы  $b^t \equiv 1$ , что невозможно, так как период числа  $a$  охватывает все числа,  $t$ -я степень которых

---

\* Разумеется, нам не обязательно знать сами эти степени, так как наименьший вычет каждой из них легко может быть получен из наименьшего вычета предыдущей степени.

сравнима с единицей (п. 53). Если  $u = p - 1$ , то  $b$  будет первообразным корнем; если же  $u$  хотя и не равно  $p - 1$ , но является кратностью  $t$ , то мы имеем уже, следовательно, число, принадлежащее большему показателю, и потому оказываемся ближе к нашей цели, состоящей в отыскании числа, принадлежащего наибольшему показателю. А если  $u$  и не равно  $p - 1$  и не кратно  $t$ , то мы все же можем найти число, которое принадлежит показателю, большему, чем  $t$  и  $u$ , а именно, показателю, равному наименьшему общему кратному чисел  $t$  и  $u$ . Если этот показатель равен  $y$ , то разложим  $y$  на два взаимно простых сомножителя  $m$  и  $n$ , причем так, что один из них входит в  $t$ , а другой входит в  $u$  \*. Если тогда  $a^{t/m} \equiv A$ ,  $b^{u/n} \equiv B \pmod{p}$ , то произведение  $AB$  будет числом, принадлежащим показателю  $y$ . Действительно, легко убедиться, что  $A$  принадлежит показателю  $m$ , а  $B$  — показателю  $n$ ; поэтому произведение  $AB$  принадлежит показателю  $mn$ , ибо  $m$  и  $n$  взаимно просты, что можно доказать совершенно тем же способом, которым в п. 55 доказывалось предложение II.

3. Если теперь  $y = p - 1$ , то  $AB$  будет первообразным корнем. Если же это не так, то нужно, аналогично тому, как раньше, взять другое число, не содержащееся в периоде числа  $AB$ . Оно или будет первообразным корнем, или будет принадлежать показателю, который больше, чем  $y$ , или по крайней мере при помощи него можно будет найти (как и перед этим) число, принадлежащее показателю, большему, чем  $y$ . Так как числа, которые получаются при повторном произведении этой операции, принадлежат ко все бóльшим и бóльшим показателям, ясно, что в конце концов будет найдено число, принадлежащее наибольшему показателю, т. е. первообразный корень.

---

\* То, как именно это можно сделать, легко получается из п. 18. Разложим  $y$  на такие сомножители, которые являются либо различными простыми числами, либо степенями различных простых чисел. Каждый из этих сомножителей входит в одно из чисел  $t$  и  $u$  (а может быть и в оба). Напишем каждый из сомножителей либо рядом с числом  $t$ , либо рядом с числом  $u$  в зависимости от того, в какое из них он входит. Если же он входит в оба эти числа, то безразлично, рядом с которым из них его писать. Если произведение сомножителей, которые написаны рядом с  $t$ , равно  $m$ , а второе произведение равно  $n$ , то легко видеть, что  $m$  входит в  $t$ , а  $n$  — в  $u$ , и что  $mn = y$ .

## 74

При разборе примера эти предписания станут более ясными. Пусть число, для которого нужно найти первообразный корень, есть  $p = 73$ . Испробуем сначала число 2, период которого оказывается следующим:

1, 2, 4, 8, 16, 32, 64, 55, 37, 1, . . .

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, . . .

Так как уже степень с показателем 9 сравнима с единицей, число 2 не является первообразным корнем. Рассмотрим поэтому какое-нибудь другое число, не содержащееся в периоде числа 2, например, 3, период которого есть

1, 3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1, . . .

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, . . .

Поэтому 3 также не является первообразным корнем. Наименьшее общее кратное чисел 9 и 12, являющихся показателями, которым принадлежат 2 и 3, есть 36, и будучи разложенным в соответствии с предписанием предыдущего пункта, оно дает сомножители 9 и 4. Умножим теперь 2 на третью степень числа 3. Произведение, равное 54, будет принадлежать показателю 36. Если, наконец, вычислить период числа 54 и снова испытать какое-нибудь не содержащееся в нем число, например, 5, то оно окажется первообразным корнем.

### Различные теоремы о периодах и первообразных корнях

## 75

Прежде чем оставить этот предмет, мы хотим добавить еще некоторые теоремы, которые представляются достойными внимания вследствие своей простоты.

*Произведение всех членов периода любого числа  $\equiv +1$ , если количество их, т. е. показатель, которому это число принадлежит, нечетно, и  $\equiv -1$ , если этот показатель четен.*

**Пример.** Для модуля 13 период числа 5 состоит из членов 1, 5, 12, 8, для произведения которых имеет место  $480 \equiv -1 \pmod{13}$ .

Период числа 3 по этому же самому модулю состоит из членов 1, 3, 9, и их произведение  $27 \equiv 1 \pmod{13}$ .

**Доказательство.** Если показатель, которому принадлежит число, равен  $t$ , а индекс самого числа есть  $(p-1)/t$ , чего, согласно п. 71, всегда можно добиться посредством выбора соответствующего основания, то индекс произведения всех членов периода

$$\equiv (1 + 2 + 3 + \dots + t - 1) \frac{p-1}{t} = \frac{(t-1)(p-1)}{2},$$

т. е.  $\equiv 0 \pmod{p-1}$ , если  $t$  нечетно, и  $\equiv (p-1)/2$ , если  $t$  четно. Поэтому в первом случае это произведение  $\equiv 1 \pmod{p}$ , а во втором  $\equiv -1 \pmod{p}$  (п. 62).

## 76

Если в предыдущей теореме число является первообразным корнем, то его период охватывает все числа 1, 2, 3, ...,  $p-1$ , произведение которых тем самым всегда  $\equiv -1$  (действительно.  $p-1$  всегда четно, за исключением одного случая  $p=2$ , когда  $-1$  и  $+1$  эквивалентны).

Эта изящная теорема, которая обычно высказывается так: *произведение всех чисел, меньших заданного простого числа, увеличенное на единицу, делится на это простое число*, была впервые опубликована Варингом и приписана им Вильсону («*Meditationes algebraicae*», ed. 3, p. 380). Однако ни тот, ни другой не могли ее доказать, и Варинг считал, что доказательство является тем более трудным, что нельзя себе представить, чтобы было такое обозначение, которое задавало бы простое число. По нашему мнению, однако, подобные истины следует черпать не из обозначений, а из понятий.

Позже доказательство дал Лагранж («*Nouv. Mém. de l'Académie de Berlin*», 1771). Оно основывается на рассмотрении коэффициентов, которые получаются при раскрытии скобок в произведении

$$(x+1)(x+2)(x+3)\dots(x+p-1).$$

Именно, если записать это произведение в виде

$$x^{p-1} + Ax^{p-2} + Bx^{p-3} + \dots + Mx + N,$$

то коэффициенты  $A, B, \dots, M$  будут делиться на  $p$ , в то время как  $N = 1 \cdot 2 \cdot 3 \dots (p-1)$ . Но при  $x = 1$  произведение делится на  $p$ ; с другой стороны, оно  $\equiv 1 + N \pmod{p}$ , и потому  $1 + N$  обязательно должно делиться на  $p$ .

Наконец, Эйлер в «*Opusc. Analyt.*», Т. 1, р. 329 дал доказательство, которое совпадает с приведенным нами. Так как такие люди не считали эту теорему недостойной своих размышлений, мы надеемся не вызвать порицания за то, что приведем еще одно ее доказательство.

## 77

Если произведение двух чисел  $a$  и  $b$  сравнимо по модулю  $p$  с единицей, то, следуя Эйлеру, мы будем называть эти числа  $a$  и  $b$  ассоциированными. Тогда, согласно предыдущему разделу, каждое положительное число, меньшее  $p$ , имеет среди положительных и меньших  $p$  чисел одно и только одно ассоциированное. Но легко доказать, что среди чисел  $1, 2, 3, \dots$  только 1 и  $p-1$  ассоциированы сами с собой. Действительно, ассоциированные сами с собой числа являются корнями сравнения  $x^2 \equiv 1$ , которое имеет вторую степень и потому не может иметь более двух корней, т. е. не имеет других корней, кроме 1 и  $p-1$ . Поэтому, если эти два числа отбросить, то остальные числа  $2, 3, \dots, p-2$  будут попарно ассоциированы и потому их произведение  $\equiv 1$ . Таким образом, произведение всех чисел, именно  $1 \cdot 2 \cdot 3 \dots (p-1) \equiv p-1$  или  $\equiv -1$ .

Например, по модулю 13 среди чисел  $2, 3, 4, \dots, 11$  ассоциированными одно с другим будут следующие: 2 и 7, 3 и 9, 4 и 10, 5 и 8, 6 и 11; действительно,  $2 \cdot 7 \equiv 1$ ,  $3 \cdot 9 \equiv 1$  и т. д. Поэтому  $2 \cdot 3 \cdot 4 \dots 11 \equiv 1$ , откуда  $1 \cdot 2 \cdot 3 \dots 12 \equiv -1$ .

## 78

В более общем виде теорему Вильсона можно высказать так. Произведение всех чисел, которые меньше некоторого заданного

числа  $A$  и одновременно взаимно просты с ним, сравнимо по модулю  $A$  с единицей, взятой с положительным или с отрицательным знаком. С отрицательным знаком единица получается, когда  $A$  имеет вид  $p^m$  или  $2p^m$ , где  $p$  обозначает отличное от 2 простое число, и, кроме того, при  $A = 4$ , во всех же остальных случаях получается положительная единица. Теорема, высказанная Вильсоном, содержится в первом случае. Например, для  $A = 15$  произведение чисел 1, 2, 4, 7, 8, 11, 13, 14 сравнимо с 1 по модулю 15. Доказательство мы ради краткости не приводим; заметим только, что оно может быть проведено подобным же образом, как в предыдущем пункте, с той только разницей, что сравнение  $x^2 \equiv 1$  может иметь и более двух корней, которые требуют некоторых специальных рассматриваний. Можно было бы также вывести доказательство из рассмотрения индексов, подобно п. 75, если принять во внимание то, что сейчас будет сказано о составных модулях.

## 79

Теперь мы возвращаемся к перечислению остальных теорем (п. 75).

*Сумма всех членов периода любого числа  $\equiv 0$ .* Так, в примере из п. 75 будем иметь  $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$ .

**Доказательство.** Если число, о периоде которого идет речь, равно  $a$ , и показатель, которому оно принадлежит, равен  $t$ , то сумма всех членов периода

$$\equiv 1 + a + a^2 + a^3 + \dots + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}.$$

Но  $a^t - 1 \equiv 0$ ; следовательно, эта сумма  $\equiv 0$  (п. 22), если только  $a - 1$  не делится на  $p$ , т. е.  $a$  не сравнимо с 1. Этот случай мы должны, таким образом, исключить, если мы хотим называть периодом также и один единственный член.

## 80

*Произведение всех первообразных корней  $\equiv 1$ ,* если исключить случай  $p = 3$ , когда имеется только один первообразный корень 2.



**Доказательство.** Если любой первообразный корень взят за основание, то индексами всех других первообразных корней будут числа, которые взаимно просты с  $p-1$  и одновременно меньше  $p-1$ . Но сумма этих чисел, т. е. индекс произведения всех первообразных корней  $\equiv 0 \pmod{p-1}$ , и потому само произведение  $\equiv 1 \pmod{p}$ ; действительно, легко видеть, что если  $k$  есть число, взаимно простое с  $p-1$ , то и  $p-1-k$  будет взаимно просто с  $p-1$ , и каждые два таких взаимно простых с  $p-1$  числа образуют сумму, которая делится на  $p-1$  ( $k$  никогда не может быть равно  $p-1-k$ , кроме случая  $p-1=2$  или  $p=3$ , который мы исключили; в самом деле, во всех остальных случаях  $(p-1)/2$ , очевидно, не взаимно просто с  $p-1$ ).

## 81

*Сумма всех первообразных корней или  $\equiv 0$  (когда  $p-1$  делится на какой-нибудь квадрат), или  $\equiv \pm 1 \pmod{p}$  (когда  $p-1$  есть произведение различных простых чисел; при этом следует брать положительный или отрицательный знак в зависимости от того, четно или нечетно число этих простых чисел).*

**Пример.** 1) Для  $p=13$  мы имеем первообразные корни 2, 6, 7, 11, сумма которых  $26 \equiv 0 \pmod{p}$ ; 2) для  $p=11$  первообразные корни суть 2, 6, 7, 8, и сумма их  $23 \equiv +1 \pmod{11}$ ; 3) для  $p=31$  первообразные корни суть 3, 11, 12, 13, 17, 21, 22, 24, и сумма их  $123 \equiv -1 \pmod{31}$ .

**Доказательство.** Мы доказали выше (п. 55, II), что если  $p-1 = a^\alpha b^\beta c^\gamma \dots$  (где  $a, b, c, \dots$  — различные простые числа) и  $A, B, C, \dots$  суть какие-нибудь числа, принадлежащие соответственно показателям  $a^\alpha, b^\beta, c^\gamma, \dots$ , то произведение  $ABC \dots$  представляет собой первообразный корень. Но легко также доказать, что каждый первообразный корень может быть представлен в виде такого произведения, и притом одним единственным способом\*.

---

\* Именно, определим числа  $a, b, c, \dots$  так, что  $a \equiv 1 \pmod{a^\alpha}$  и  $\equiv 0 \pmod{b^\beta c^\gamma \dots}$ ,  $b \equiv 1 \pmod{b^\beta}$  и  $\equiv 0 \pmod{a^\alpha c^\gamma \dots}$ , и т. д. (ср. п. 32). Тогда  $a + b + c + \dots \equiv 1 \pmod{p-1}$  (п. 19). Если теперь какой-нибудь первообразный корень  $r$  нужно представить в виде произведения  $ABC \dots$ , то

Отсюда следует, что вместо первообразных корней можно брать эти произведения. Но так как в этих произведениях всевозможные значения  $A$  должны комбинироваться со всевозможными значениями  $B$  и т. д., то сумма всех этих произведений равна произведению суммы всевозможных значений  $A$  на сумму всевозможных значений  $B$ , на сумму всевозможных значений  $C$  и т. д., что показывается в комбинаторике. Если обозначить всевозможные значения  $A, B, \dots$  соответственно через  $A, A', A'', \dots, B, B', B'', \dots, \dots$ , то сумма всех первообразных корней будет

$$\equiv (A + A' + A'' + \dots)(B + B' + B'' + \dots) \dots$$

Я утверждаю теперь, что если показатель  $\alpha = 1$ , то сумма  $A + A' + A'' + \dots \equiv -1 \pmod{p}$ , а если  $\alpha > 1$ , то эта сумма  $\equiv 0$ , и так же обстоит дело для  $\beta, \gamma, \dots$ . Если это будет доказано, то отсюда будет сразу вытекать справедливость нашей теоремы. Действительно, если  $p - 1$  делится на некоторый квадрат, то какой-нибудь из показателей  $\alpha, \beta, \gamma, \dots$  будет превосходить единицу, и потому какой-нибудь из сомножителей, с произведением которых сравнима сумма первообразных корней,  $\equiv 0$ , а значит  $\equiv 0$  и само произведение. Если же  $p - 1$  не делится ни на какой квадрат, то все показатели  $\alpha, \beta, \gamma, \dots$  будут равны 1; поэтому сумма всех первообразных корней будет сравнима с произведением такого количества сомножителей (каждый из которых  $\equiv -1$ ), сколько имеется чисел  $a, b, c, \dots$ , т. е.  $\equiv \pm 1$  в зависимости от того, четно или нечетно число этих чисел. Указанные же выше утверждения доказываются следующим образом.

1. Если  $\alpha = 1$  и  $A$  — число, принадлежащее показателю  $a$ , то остальными числами, принадлежащими этому показателю, будут  $A^2, A^3, \dots, A^{a-1}$ . Но

$$1 + A + A^2 + A^3 + \dots + A^{a-1}$$

является суммой полного периода и потому  $\equiv 0 \pmod{p}$  (п. 79); поэтому

$$A + A^2 + A^3 + \dots + A^{a-1} \equiv -1.$$

---

положим  $A \equiv r^a, B \equiv r^b, C \equiv r^c, \dots$ ; тогда  $A$  будет принадлежать показателю  $a^a$ ,  $B$  — показателю  $b^b$  и т. д., и произведение всех чисел  $A, B, C, \dots$  будет  $\equiv r \pmod{p}$ . Легко видеть также, что числа  $A, B, C, \dots$  не могут иметь никаких других значений, кроме указанных.

2. Если же  $\alpha > 1$  и  $A$  — число, принадлежащее показателю  $a^\alpha$ , то другие принадлежащие этому показателю числа мы получим, если из чисел  $A^2, A^3, A^4, \dots, A^{a^\alpha-1}$  отбросим числа  $A^a, A^{2a}, A^{3a}, \dots$  (ср. п. 53). Поэтому их сумма

$$\equiv 1 + A + A^2 + \dots + A^{a^\alpha-1} - (1 + A^a + A^{2a} + \dots + A^{a^\alpha-a}),$$

т. е. сравнима с разностью двух периодов и потому  $\equiv 0$ .

### О модулях, которые являются степенями простых чисел

#### 82

Все, что мы изложили до сих пор, основывается на предположении, что модуль является простым числом. Остается еще рассмотреть случай, когда *за модуль берется составное число*. Так как, однако, появляющиеся здесь теоремы не столь изящны, как в первом случае, и для их обнаружения не требуется особенно тонких приемов, а можно их вывести простым применением ранее изложенных принципов, то было бы и утомительным и излишним разбирать здесь все подробности. Поэтому мы лишь кратко изложим, что этот случай имеет общего с предыдущим и в чем от него отличается.

#### 83

Теоремы пп. 45—48 были уже доказаны для общего случая; теорему же из п. 49 нужно изменить следующим образом.

*Если через  $f$  обозначить количество чисел, которые меньше  $t$  и одновременно взаимно просты с  $t$ , т. е. если  $f = \varphi(t)$  (п. 38), то для заданного взаимно простого с  $t$  числа  $a$  показатель  $t$  наинизшей его степени, которая сравнима с единицей по модулю  $t$ , или равен  $f$ , или является делителем этого числа.*

Доказательство теоремы из п. 49 проходит и в этом случае, если только взять  $t$  вместо  $p$ ,  $f$  вместо  $p-1$ , а вместо чисел  $1, 2, 3, \dots, p-1$  — те числа, которые взаимно просты с  $t$  и одновременно мень-

ше  $m$ . Поэтому мы предоставляем это читателю. Впрочем, и другие доказательства, о которых мы там (пп. 50, 51) говорили, без больших изменений переносятся на этот случай. Однако, в отношении следующих теорем (п. 52 и далее) имеется большое различие между модулями, которые являются степенями простых чисел, и теми, которые делятся на несколько простых чисел. Мы рассмотрим поэтому модули первого типа отдельно.

## 84

Если модуль  $m = p^n$ , где  $p$  — простое число, то  $f = p^{n-1}(p - 1)$  (п. 38). Если теперь применить к этому случаю исследования в пп. 53, 54, то, внося изменения, указанные в предыдущем пункте, мы убедимся, что все доказанное там верно и в этом случае, если только доказать сначала, что сравнение вида  $x^t - 1 \equiv 0 \pmod{p^n}$  не может иметь больше чем  $t$  корней. Для простого модуля мы вывели этот факт из общей теоремы п. 43, которая, однако, в общем виде верна только для простых модулей, и потому в рассматриваемом сейчас случае не может быть применена. Однако мы докажем особым методом, что для данного частного случая теорема верна. В дальнейшем (раздел VIII) мы научимся доказывать это проще.

## 85

Мы хотим доказать следующую теорему.

*Если  $e$  есть наибольший общий делитель чисел  $t$  и  $p^{n-1}(p - 1)$  то сравнение  $x^t \equiv 1 \pmod{p^n}$  имеет  $e$  различных корней.*

Пусть  $e = kp^v$ , где  $k$  не содержит сомножителем  $p$  и потому входит в  $p - 1$ . Тогда сравнение  $x^t \equiv 1 \pmod{p}$  будет иметь  $k$  различных корней, и если обозначить их через  $A, B, C, \dots$ , то каждый корень такого же сравнения по модулю  $p^n$  должен быть сравним по модулю  $p$  с одним из чисел  $A, B, C, \dots$ . Теперь мы докажем, что сравнение  $x^t \equiv 1 \pmod{p^n}$  имеет  $p^v$  корней, сравнимых с  $A$ , столько же корней, сравнимых с  $B$ , и т. д. по модулю  $p$ . Отсюда будет следовать, что количество всех корней равно  $kp^v$ , т. е. равно  $e$ , что и утверждается. Указанное доказательство мы

проведем следующим образом. Во-первых, мы покажем, что если  $\alpha$  есть корень, сравнимый с  $A$  по модулю  $p$ , то корнями будут также и  $\alpha + p^{n-\nu}$ ,  $\alpha + 2p^{n-\nu}$ ,  $\alpha + 3p^{n-\nu}$ , ...,  $\alpha + (p^\nu - 1)p^{n-\nu}$ ; во-вторых, что среди чисел, сравнимых с  $A$  по модулю  $p$ , нет других корней, кроме тех, которые имеют вид  $\alpha + hp^{n-\nu}$  (где  $h$  обозначает произвольное целое число), откуда следует, что имеется  $p^\nu$ , но не больше, таких корней. То же самое имеет место и для корней, сравнимых с числами  $B, C, \dots$ ; в-третьих, мы покажем, что всегда можно найти один корень, который сравним с  $A$  по модулю  $p$ .

86

**Теорема.** Если  $t$ , как и в предыдущем пункте, есть число, которое делится на  $p^\nu$ , но не делится на  $p^{\nu+1}$ , то

$$(\alpha + hp^\mu)^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}} \text{ или } \equiv \alpha^{t-1}hp^\mu t \pmod{p^{\mu+\nu+1}}.$$

Вторая часть теоремы не верна, если  $p = 2$  и одновременно  $\mu = 1$ .

Доказательство этой теоремы можно было бы вывести из разложения степени бинорма, если показать, что все члены после второго делятся на  $p^{\mu+\nu+1}$ . Так как, однако, рассмотрение знаменателей коэффициентов приводит к некоторым затруднениям, мы вместо этого применим следующий метод.

Если мы сначала предположим, что  $\mu > 1$  и  $\nu = 1$ , то так как

$$x^t - y^t = (x - y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \dots + y^{t-1}),$$

имеет место

$$(\alpha + hp^\mu)^t - \alpha^t = hp^\mu [(\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha + \dots + \alpha^{t-1}].$$

Но

$$\alpha + hp^\mu \equiv \alpha \pmod{p^2}.$$

Поэтому каждый член  $(\alpha + hp^\mu)^{t-1}$ ,  $(\alpha + hp^\mu)^{t-2}$ , ...,  $\equiv \alpha^{t-1} \pmod{p^2}$ , и значит сумма их всех  $\equiv t\alpha^{t-1} \pmod{p^2}$ , т. е. имеет вид  $t\alpha^{t-1} + vp^2$ , где  $v$  есть некоторое число. Следовательно,  $(\alpha + hp^\mu)^t - \alpha^t$  будет иметь вид

$$\alpha^{t-1}hp^\mu t + vhp^{\mu+2}, \text{ т. е. } \equiv \alpha^{t-1}hp^\mu t \pmod{p^{\mu+2}} \text{ и } \equiv 0 \pmod{p^{\mu+1}}.$$

Тем самым для этого случая теорема доказана.

Если теперь по-прежнему остается  $\mu > 1$ , но для других значений  $\nu$  теорема не верна, то обязательно должна существовать граница, до которой теорема все время верна, а за ней уже становится неверной. Пусть наименьшее значение  $\nu$ , для которого она больше не верна, равно  $\varphi$ . Тогда легко видеть, что если  $t$  делится на  $p^{\varphi-1}$ , но не делится на  $p^{\varphi}$ , то теорема еще верна, но перестает быть верной, если  $t$  заменить на  $tp$ . Поэтому

$$(\alpha + hp^{\mu})^t \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\varphi}} \text{ или } \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi},$$

где  $u$  означает целое число. Но так как для  $\nu = 1$  теорема уже доказана, мы имеем

$$\begin{aligned} & (\alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi})^p \equiv \\ & \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-t}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}, \end{aligned}$$

и потому также

$$(\alpha + hp^{\mu})^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu}tp \pmod{p^{\mu+\varphi+1}},$$

т. е. теорема верна и при замене  $t$  на  $tp$ , т. е. верна для  $\nu = \varphi$ , что находится в противоречии с нашим предположением. Отсюда следует, что теорема верна для всех значений  $\nu$ .

Остается еще случай, когда  $\mu = 1$ . При помощи метода, совершенно аналогичного тому, который применялся в предыдущем пункте, можно, не прибегая к помощи биномиальной теоремы, доказать, что

$$\begin{aligned} & (\alpha + hp)^{t-1} \equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}, \\ & \alpha(\alpha + hp)^{t-2} \equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp, \\ & \alpha^2(\alpha + hp)^{t-3} \equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp, \\ & \dots \dots \dots \end{aligned}$$

так что многочлен (ибо число слагаемых равно  $t$ ) будет

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2} \alpha^{t-2} hp \pmod{p^2}.$$

Но так как  $t$  делится на  $p$ , то и  $(t-1)t/2$  будет делиться на  $p$  во всех случаях, за исключением случая  $p=2$ , который мы исключили из рассмотрения еще в предыдущем пункте. В остальных же случаях будет иметь место  $\frac{(t-1)t}{2} \alpha^{t-2} hp \equiv 0 \pmod{p^2}$ , и потому указанный многочлен будет, как и в предыдущем пункте  $\equiv t\alpha^{t-1} \pmod{p^2}$ . В остальном доказательство здесь проводится точно так же, как и там.

Поэтому мы можем сделать вывод, что, за исключением случая  $p=2$ , всегда имеет место

$$(\alpha + hp^\mu)^t \equiv \alpha^t \pmod{p^{\mu+\nu}},$$

и  $(\alpha + hp^\mu)^t$  несравнимо с  $\alpha^t$  для каждого модуля, являющегося более высокой степенью  $p$ , чем  $p^{\mu+\nu}$ , где предполагается, что  $h$  не делится на  $p$ , и  $p^\nu$  есть наивысшая входящая в  $t$  степень  $p$ .

Отсюда тотчас же вытекают утверждения 1 и 2, которые мы наметили для доказательства в п. 85. Именно,

*во-первых*, если  $\alpha^t \equiv 1$ , то и  $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$ ,

*во-вторых*, предположим, что какое-нибудь число  $\alpha'$ , сравнимое по модулю  $p$  с  $A$ , а поэтому и с  $\alpha$ , но несравнимое с последним по модулю  $p^{n-\nu}$ , удовлетворяет сравнению  $x^t \equiv 1 \pmod{p^n}$ , и положим  $\alpha' = \alpha + lp^\lambda$ , где  $l$  не делится на  $p$  и  $\lambda < n - \nu$ ; тогда  $(\alpha + lp^\lambda)^t \equiv \alpha^t$  по модулю  $p^{\lambda+\nu}$ , но не по модулю  $p^n$ , который является более высокой степенью  $p$ . Поэтому в действительности  $\alpha'$  не может быть корнем сравнения  $x^t \equiv 1$ .

*В-третьих*, мы должны были найти какой-нибудь один корень сравнения  $x^t \equiv 1 \pmod{p^n}$ , который сравним с  $A$ . Мы здесь покажем только, как это можно сделать, если уже известен корень такого же сравнения по модулю  $p^{n-1}$ . Очевидно, что этого достаточно, потому что мы сможем тогда перейти от модуля  $p$ , для

которого корнем является  $A$ , к модулю  $p^2$  и точно так же ко всем последующим степеням.

Итак, пусть  $\alpha$  — корень сравнения  $x^t \equiv 1 \pmod{p^{n-1}}$ , и надо найти корень этого сравнения по модулю  $p^n$ . Положим его равным  $\alpha + hp^{n-v-1}$ ; эту форму он должен иметь согласно предыдущему пункту (случай, когда  $v = n - 1$  мы затем рассмотрим отдельно; больше же, чем  $n - 1$ ,  $v$  быть не может). Таким образом, должно быть

$$(\alpha + hp^{n-v-1})^t \equiv 1 \pmod{p^n}.$$

Но

$$(\alpha + hp^{n-v-1})^t \equiv \alpha^t + \alpha^{t-1} htp^{n-v-1} \pmod{p^n}.$$

Поэтому, если определить  $h$  так, что  $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-v-1} \pmod{p^n}$  или (ибо, по предположению,  $1 \equiv \alpha^t \pmod{p^{n-1}}$  и  $t$  делится на  $p^v$ )

так, что  $\frac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1} h \frac{t}{p^v}$  делится на  $p$ , то мы и получим то,

что нам нужно. А то, что это всегда возможно, вытекает из предыдущего раздела, так как мы предположили, что  $t$  не должно делиться на более высокую степень  $p$  чем  $p^v$ , и потому  $\alpha^{t-1}t/p^v$  взаимно просто с  $p$ .

Если же  $v = n - 1$ , т. е. если  $t$  делится на  $p^{n-1}$  или на еще бóльшую степень  $p$ , то каждое значение  $A$ , которое удовлетворяет уравнению  $x^t \equiv 1$  по модулю  $p$ , будет удовлетворять ему и по модулю  $p^n$ . Действительно, если  $t = p^{n-1}\tau$ , то  $t \equiv \tau \pmod{p-1}$ ; поэтому, так как  $A^t \equiv 1 \pmod{p}$ , то и  $A^\tau \equiv 1 \pmod{p}$ . Следовательно, если положить  $A^\tau = 1 + hp$ , то

$$A^t = (1 + hp)^{p^{n-1}} \equiv 1 \pmod{p^n} \text{ (п. 87).}$$

Все, что в пп. 57 и следующих мы вывели при помощи теоремы, что сравнение  $x^t \equiv 1$  не может иметь более чем  $t$  различных корней, сохраняет силу также и для модуля, являющегося степенью простого числа; и если мы назовем **первообразными корнями** те числа, которые принадлежат показателю  $p^{n-1}(p-1)$ , или те, в периодах которых содержатся все числа, не делящиеся на  $p$ , то и в этом случае первообразные корни будут существовать.



Далее, все, что мы говорили выше относительно индексов и их применений, а также относительно решения сравнения  $x^t \equiv 1$ , может применяться также и в этом случае. Так как никаких трудностей здесь нет, было бы излишне все это полностью повторять. Кроме того, мы уже показали, как можно получать корни сравнения  $x^t \equiv 1$  по модулю  $p^n$  из корней этого сравнения по модулю  $p$ . Мы должны добавить кое-что относительно случая, когда модулем является некоторая степень числа 2 — случая, который выше мы из рассмотрения исключали.

### Модули, являющиеся степенями числа 2

#### 90

*Если за модуль взята некоторая степень  $2^n$  числа 2, бóльшая, чем вторая, то степень каждого нечетного числа с показателем  $2^{n-2}$  сравнима с единицей.*

Например,  $3^8 = 6561 \equiv 1 \pmod{32}$ .

Действительно, каждое нечетное число имеет вид или  $1 + 4h$ , или  $-1 + 4h$ , откуда теорема следует непосредственно (теорема из п. 86).

Так как, таким образом, показатель, которому принадлежит любое нечетное число по модулю  $2^n$ , является делителем числа  $2^{n-2}$ , то каждое число должно принадлежать одному из следующих показателей:  $1, 2, 4, 8, \dots, 2^{n-2}$ . Какому именно из них оно принадлежит, легко можно определить следующим образом. Если данное число равно  $4h \pm 1$ , и показатель наибольшей степени числа 2, входящей в  $h$ , равен  $m$  (где  $m$  может быть и равным 0, именно, когда  $h$  нечетно), то в случае  $h > m + 2$  показатель, которому принадлежит данное число, равен  $2^{n-m-2}$ . Если же  $n$  равно или меньше, чем  $m + 2$ , то заданное число  $\equiv \pm 1$  и потому принадлежит показателю 1 или показателю 2. Действительно, как без труда вытекает из п. 86, каждое число вида  $\pm 1 + 2^{m+2}k$  (что эквивалентно виду  $4h \pm 1$ ), возведенное в степень с показателем  $2^{n-m-2}$ , сравнимо с единицей по модулю  $2^n$ ; если же возвести это число в степень с показателем, являющимся более низкой степенью

числа 2, то оно с единицей сравнимо не будет. Поэтому каждое число вида  $8k + 3$  или  $8k + 5$  принадлежит показателю  $2^{n-2}$ .

## 91

Из сказанного вытекает, что в этом случае не существует первообразных корней в том смысле, в котором мы употребляли это выражение выше, т. е. не существует чисел, периоды которых охватывают все числа, меньшие модуля и взаимно простые с ним. Однако легко видеть, что некоторая аналогия имеется и здесь. Именно, оказывается, что степень числа вида  $8k + 3$  с нечетным показателем всегда имеет вид  $8k + 3$ , а степень с четным показателем — вид  $8k + 1$ ; таким образом, никакая степень не может быть вида  $8k + 5$  или  $8k + 7$ . Так как, таким образом, период числа вида  $8k + 3$  состоит из  $2^{n-2}$  различных членов, каждый из которых имеет вид  $8k + 1$  или вид  $8k + 3$ , и среди чисел, меньших модуля, чисел такого вида не может быть больше, чем  $2^{n-2}$ , то ясно, что каждое число вида  $8k + 1$  или  $8k + 3$  сравнимо по модулю  $2^n$  с некоторой степенью любого числа вида  $8k + 3$ . Аналогичным образом можно показать, что период числа вида  $8k + 5$  содержит все числа вида  $8k + 1$  или  $8k + 5$ . Поэтому, если за основание взято число вида  $8k + 5$ , то все числа вида  $8k + 1$  и  $8k + 5$ , взятые положительными, и все числа вида  $8k + 3$  и  $8k + 7$ , взятые отрицательными, будут иметь вещественные индексы, причем индексы, сравнимые по модулю  $2^{n-2}$ , следует рассматривать как эквивалентные. В этом смысле надо понимать нашу таблицу 1\*, в которой мы для модулей 16, 32 и 64 (для модуля 8 таблицы, конечно, не нужно) всегда брали за основание число 5. Например, для модуля 64 числу 19, которое имеет вид  $8n + 3$  и потому должно браться отрицательным, соответствует индекс 7, что означает, что  $5^7 \equiv -19 \pmod{64}$ . Взатым отрицательными числам вида  $8n + 1$  и  $8n + 5$  и взатым положительными числам вида  $8n + 3$  и  $8n + 7$  можно было бы определенным образом сопоставить мнимые индексы. Если бы их ввести, то действия с индексами можно было бы свести к очень простому алгоритму.

\* Таблица помещена на стр. 576.— *Прим. ред.*

Но так как мы были бы заведены слишком далеко, если бы захотели изложить это с полнейшей строгостью, мы оставим это до другого случая, когда мы будем излагать теорию мнимых величин, которая, по нашему мнению, до сих пор еще никем не была приведена к ясным понятиям. Имеющие навык легко найдут этот алгоритм сами; впрочем, для того, чтобы употреблять эту таблицу, нужен лишь небольшой опыт, подобно тому как те, кому не известны новейшие исследования о мнимых логарифмах, могут пользоваться логарифмами, если они только поняли изложенные выше принципы.

### Модули, составленные из нескольких простых чисел

#### 92

В отношении модулей, составленных из нескольких простых чисел, почти все, касающееся вычетов степеней, может быть выведено из общей теории сравнений. Так как, однако, впоследствии мы более подробно будем показывать, как любые сравнения по модулям, составленным из нескольких простых чисел, могут быть сведены к сравнениям, модули которых суть простые числа или степени простых чисел, здесь нам нет нужды долго задерживаться на этом предмете. Заметим только, что красивое свойство, существующее для модулей, которые суть простые числа или степени простых чисел, именно, что всегда существуют числа, периоды которых содержат все числа, взаимно простые с модулем, здесь уже не имеет места, за исключением того случая, когда модуль есть удвоенное простое число или удвоенная степень простого числа. Именно, если модуль  $m$  имеет вид  $A^a B^b C^c \dots$ , где  $A, B, C, \dots$  обозначают различные простые числа, далее,  $A^{a-1}(A-1)$  обозначается через  $\alpha$ ,  $B^{b-1}(B-1)$  — через  $\beta$ , и т. д., и наконец,  $z$  есть число, взаимно простое с  $m$ , то  $z^\alpha \equiv 1 \pmod{A^a}$ ,  $z^\beta \equiv 1 \pmod{B^b}$  и т. д. Если теперь  $\mu$  есть наименьшее общее кратное чисел  $\alpha, \beta, \gamma, \dots$ , то сравнение  $z^\mu \equiv 1$  будет выполняться по всем модулям  $A^a, B^b, \dots$ , а потому и по модулю  $m$ , являющемуся их произведением. Но за исключением случая, когда  $m$  есть удвоенное простое число или удвоенная степень простого числа, наименьшее общее кратное

чисел  $\alpha, \beta, \gamma, \dots$  меньше их произведения (так как числа  $\alpha, \beta, \gamma, \dots$  не могут быть взаимно просты, ибо обязательно содержат общий делитель 2). Поэтому ни у какого числа период не содержит столько членов, сколько имеется чисел, взаимно простых с модулем и меньших модуля, так как это количество равно произведению чисел  $\alpha, \beta, \gamma, \dots$ . Так, например, для  $m = 1001$  шестидесятая степень каждого числа, взаимно простого с  $m$ , сравнима с единицей, потому что 60 есть наименьшее общее кратное чисел 6, 10, 12. Случай же, когда модуль есть удвоенное простое число или удвоенная степень простого числа, совершенно аналогичен тому, когда модуль есть простое число или его степень.

## 93

Работы, в которых другие математики касались изложенного здесь предмета, мы уже упоминали мимоходом. Тех, которые хотели бы ознакомиться с этим предметом несколько более подробно, чем мы, из желания быть краткими, сообщили здесь, мы отсылаем в первую очередь к следующим сочинениям Эйлера, которые особенно достойны быть рекомендованы вследствие ясности изложения, всегда отличающей этого великого человека от других математиков:

«*Theoremata circa residua ex divisione potestatum relictata*». *Comm. nov. Petrop.*, T. VII, p. 49;

*Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*». *Ibid.*, T. XVIII, p. 85.

Можно указать также на работы 5 и 8 в его «*Opusculis Analyticis*», T. I.

---

## РАЗДЕЛ IV

### О СРАВНЕНИЯХ ВТОРОЙ СТЕПЕНИ

#### Квадратичные вычеты и невычеты

94

**Теорема.** Если какое-нибудь число  $m$  взять в качестве модуля, то из чисел  $0, 1, 2, 3, \dots, m-1$  могут быть сравнимы с некоторыми квадратами не более чем  $\frac{1}{2}m + 1$  чисел, если  $m$  четно, и не более чем  $\frac{1}{2}m + \frac{1}{2}$  чисел, если  $m$  нечетно.

**Доказательство.** Так как квадраты сравнимых чисел тоже, очевидно, сравнимы, то каждое число, сравнимое с некоторым квадратом, сравнимо и с квадратом числа, меньшего чем  $m$ . Поэтому нам нужно рассмотреть только наименьшие вычеты квадратов  $0, 1, 4, 9, \dots, (m-1)^2$ . Но легко видеть, что  $(m-1)^2 \equiv 1$ ,  $(m-2)^2 \equiv 2^2$ ,  $(m-3)^2 \equiv 3^2$ , и т. д. Поэтому если  $m$  четно, то будут совпадать наименьшие вычеты квадратов  $\left(\frac{1}{2}m-1\right)^2$  и  $\left(\frac{1}{2}m+1\right)^2$ ,  $\left(\frac{1}{2}m-2\right)^2$  и  $\left(\frac{1}{2}m+2\right)^2$  и т. д.; если же  $m$  нечетно, то будут сравнимы квадраты  $\left(\frac{1}{2}m-\frac{1}{2}\right)^2$  и  $\left(\frac{1}{2}m+\frac{1}{2}\right)^2$ ,  $\left(\frac{1}{2}m-\frac{3}{2}\right)^2$  и  $\left(\frac{1}{2}m+\frac{3}{2}\right)^2$  и т. д. Отсюда вытекает, что при четном  $m$  не может быть сравнимо с квадратом ни одно из чисел, кроме тех, которые сравнимы с одним из квадратов  $0, 1, 4, 9, \dots, \left(\frac{1}{2}m\right)^2$ , а при нечетном  $m$  каж-

дое число, сравнимое с некоторым квадратом, обязательно сравнимо с одним из чисел  $0, 1, 4, 9, \dots, \left(\frac{1}{2}m - \frac{1}{2}\right)^2$ . Поэтому в первом случае имеется не больше чем  $\frac{1}{2}m + 1$ , а во втором не больше чем  $\frac{1}{2}m + \frac{1}{2}$  различных наименьших вычетов.

**Пример.** По модулю 13 квадраты чисел  $0, 1, 2, 3, \dots, 6$  имеют следующие наименьшие вычеты:  $0, 1, 4, 9, 3, 12, 10$ ; затем они снова повторяются в обратном порядке. Поэтому не может быть сравнимо с квадратом ни одно число, которое не сравнимо с одним из этих вычетов, т. е. которое сравнимо с одним из чисел  $2, 5, 6, 7, 8, 11$ .

По модулю 15 получаются следующие вычеты:  $0, 1, 4, 9, 1, 10, 6, 4$ ; затем они же повторяются в обратном порядке. Таким образом, здесь число вычетов, которые могут быть сравнимы с некоторыми квадратами, даже меньше, чем  $\frac{1}{2}m + \frac{1}{2}$ , ибо такими вычетами являются только  $0, 1, 4, 6, 9, 10$ . Числа же  $2, 3, 5, 7, 8, 11, 12, 13, 14$  и все сравнимые с ними не могут быть сравнимы по модулю 15 ни с каким квадратом.

## 95

Из сказанного следует, что для каждого модуля все числа могут быть разбиты на два класса, один из которых содержит все числа, которые сравнимы с некоторыми квадратами, а другой — те числа, для которых это не имеет места. Мы будем называть первые *квадратичными вычетами взятого в качестве модуля числа* \*, а вторые — *его квадратичными невычетами*, а когда это

---

\* Собственно говоря, мы используем здесь это выражение в другом смысле, нежели мы это делали до сих пор. Именно, мы должны были бы говорить, что  $r$  есть вычет квадрата  $a^2$  по модулю  $m$ , если  $r \equiv a^2 \pmod{m}$ . Однако ради краткости мы в этом разделе всегда будем называть  $r$  квадратичным вычетом самого числа  $m$ , не опасаясь, что это может привести к недоразумениям, так как выражение «вычет» в смысле «сравнимое число» мы, начиная отсюда, будем употреблять лишь тогда, когда речь идет о наименьшем вычете, а в этом случае никакой двусмысленности возникнуть не может.

не сможет привести к недоразумению, будем также использовать просто выражения «вычеты и невычеты». Очевидно, что если все числа  $0, 1, 2, \dots, m-1$  распределены по обоим классам, то сравнимые числа содержатся в том же классе.

В этих исследованиях мы также начнем с простых модулей; это все время будет молчаливо предполагаться, даже когда об этом и не будет специально упоминаться. При этом простое число 2 исключается, т. е. будут рассматриваться только нечетные простые числа.

**Если модуль есть простое число,  
то среди чисел, меньших его, количество вычетов  
равно количеству невычетов**

96

*Если за модуль взято простое число  $p$ , то среди чисел  $1, 2, 3, \dots, p-1$  половина будет квадратичными вычетами, а остальные — невычетами, т. е. имеется  $\frac{1}{2}(p-1)$  вычетов и столько же невычетов.*

Именно, легко доказать, что все квадраты  $1, 4, 9, \dots, \frac{1}{4}(p-1)^2$  несравнимы между собой. Действительно, если бы имело место  $r^2 \equiv r'^2 \pmod{p}$  и числа  $r$  и  $r'$  были бы не больше, чем  $(p-1)/2$ , и не равны между собой, то, предполагая  $r > r'$ , что законно, мы имели бы, что число  $(r-r')(r+r')$  положительно и делится на  $p$ . Но каждый из сомножителей  $r-r'$  и  $r+r'$  меньше  $p$ , и потому наше предположение не может иметь места (п. 13). Поэтому среди чисел  $1, 2, 3, \dots, p-1$  имеется  $(p-1)/2$  квадратичных вычетов; но больше среди этих чисел вычетов быть не может, так как, присоединяя еще вычет 0, мы уже получим  $(p+1)/2$  вычетов, а количество всех вычетов не может превосходить этого числа. Таким образом, остальные числа являются невычетами, и тем самым их количество равно  $(p-1)/2$ .

Так как нуль всегда является вычетом, то в этих исследованиях мы исключим его из рассмотрения вместе с числами, делящимися на модуль; этот случай сам по себе ясен и лишь удлиняет теоремы. На этом же основании мы исключили также и модуль 2.

Так как многое из того, что мы будем разбирать в этом разделе, может быть выведено также и на основании принципов предыдущего раздела, и так как не является бесполезным получать одну и ту же истину различными путями, мы сейчас поясним эту связь. Легко видеть, что все числа, сравнимые с некоторыми квадратами, имеют *четные индексы*, а несравнимые с квадратами — *нечетные*. Но так как  $p - 1$  есть четное число, то количество четных и нечетных индексов одинаково, именно, и тех, и других по  $(p - 1)/2$ , и столько же будет вычетов и невычетов.

### Примеры

| Для модулей | Вычетами являются         |
|-------------|---------------------------|
| 3           | 1                         |
| 5           | 1, 4                      |
| 7           | 1, 2, 4                   |
| 11          | 1, 3, 4, 5, 9             |
| 13          | 1, 3, 4, 9, 10, 12        |
| 17          | 1, 2, 4, 8, 9, 13, 15, 16 |
| ...         | ...                       |

остальные же числа, меньшие этих модулей, суть невычеты.

**Ответ на вопрос, является ли составное число вычетом или невычетом заданного простого числа, зависит от свойств сомножителей**

**Теорема.** Произведение двух квадратичных вычетов простого числа  $p$  является вычетом; произведение вычета на невычет является невычетом; наконец, произведение двух невычетов является вычетом.

**Доказательство.** I. Пусть  $A, B$  — вычеты, получающиеся из квадратов  $a^2, b^2$ , т. е.  $A \equiv a^2, B \equiv b^2$ ; тогда произведение  $AB$  будет сравнимо с квадратом числа  $ab$ , т. е. будет вычетом.



II. Если  $A$  есть вычет, например,  $\equiv a^2$ , а  $B$  — невычет, то  $AB$  будет невычетом. Действительно, если мы предположим, что  $AB \equiv k^2$  и  $\frac{k}{a} \equiv b \pmod{p}$ , то будет иметь место  $a^2 B \equiv a^2 b^2$ , и потому  $B \equiv b^2$ , т. е., вопреки нашему предположению,  $B$  будет вычетом.

**Другое доказательство.** Если все вычеты, содержащиеся среди чисел  $1, 2, 3, \dots, p-1$  (количество этих вычетов равно  $(p-1)/2$ ), умножить на  $A$ , то все произведения будут квадратичными вычетами и все будут несравнимы между собой. Если теперь умножить на  $A$  невычет  $B$ , то произведение не будет сравнимо ни с одним из ранее полученных произведений. Поэтому, если бы оно было вычетом, то мы имели бы  $(p+1)/2$  несравнимых между собой вычетов, среди которых нет нуля. Но это противоречит п. 96.

III. Если  $A$  и  $B$  — невычеты, то, умножая на  $A$  все вычеты, содержащиеся среди чисел  $1, 2, 3, \dots, p-1$ , мы, согласно II, получим  $(p-1)/2$  несравнимых между собой невычетов. Но ни одно из этих произведений не может быть сравнимо с произведением  $AB$ . Поэтому, если бы оно было невычетом, мы имели бы  $(p+1)/2$  несравнимых между собой невычетов, что противоречит п. 96.

Еще легче можно вывести эти теоремы из принципов предыдущего раздела. Действительно, так как индексы вычетов всегда четны, а индексы невычетов нечетны, то индекс произведения двух вычетов или двух невычетов будет четным, и потому само произведение есть вычет. Наоборот, индекс произведения вычета на невычет будет нечетным, и потому само произведение есть невычет.

Оба метода могут быть применены также для доказательства следующих теорем.

*Значение выражения  $\frac{a}{b} \pmod{p}$  является вычетом, если числа  $a$  и  $b$  являются одновременно или вычетами, или невычетами; наоборот, оно будет невычетом, если одно из чисел  $a$  и  $b$  есть вычет, а другое — невычет.*

Эти теоремы могут быть получены также обращением предыдущих теорем.

Вообще, произведение любого количества сомножителей есть вычет как в том случае, когда все сомножители — вычеты, так и в том, когда число невычетов среди них четно; если же число невычетов, находящихся среди сомножителей, нечетно, то произведение есть невычет. Поэтому легко можно узнать, является ли заданное число вычетом или невычетом, если мы знаем это относительно его отдельных сомножителей. Поэтому в таблицу  $2^*$  мы вносили только простые числа. Устройство этой таблицы следующее. Слева расположены столбцом модули  $**$ , в верхней строке стоят последовательные простые числа; если какое-нибудь из них является вычетом по некоторому модулю, то на пересечении соответствующих строки и столбца ставится маленькая черточка; если же простое число является невычетом модуля, то соответствующее место оставляется пустым.

### О модулях, являющихся составными числами

Прежде чем переходить к более трудным теоремам, нам нужно еще кое-что добавить относительно не простых модулей.

Если за модуль взята любая степень  $p^n$  простого числа  $p$  (мы предполагаем, что  $p$  не равно 2), то среди чисел, которые не делятся на  $p$  и меньше модуля, половина является вычетами, а остальные невычетами, т. е. количество как тех, так и других равно  $(p - 1) p^{n-1}/2$ .

Действительно, если число  $r$  есть вычет, то оно будет сравнимо с квадратом некоторого числа, не превосходящего половины модуля (ср. п. 94). Но легко видеть, что существует  $(p - 1) p^{n-1}/2$  чисел, которые не делятся на  $p$  и меньше половины модуля, и потому нужно только показать, что квадраты всех этих чисел не сравнимы один с другим, т. е. дают различные квадратичные вычеты. Но если бы квадраты двух чисел  $a$  и  $b$ , которые оба не делятся на  $p$  и меньше половины модуля, были бы сравнимы между

\* Таблица помещена на стр. 577.— *Прим. ред.*

\*\* Мы скоро покажем, как можно избавиться от составных модулей.

собой, то  $a^2b^2 = (a - b)(a + b)$  должно было бы делиться на  $p^n$  (мы предполагаем при этом  $a > b$ , что законно). Это возможно, однако, только тогда, когда либо одно из чисел  $a - b$ ,  $a + b$  делится на  $p^n$ , что не имеет места, потому что оба они меньше  $p^n$ , либо одно из этих чисел делится на  $p^m$ , а другое на  $p^{n-m}$ , т. е. оба делятся на  $p$ . Однако и этого не может быть. В самом деле, очевидно, что тогда сумма и разность этих чисел, именно  $2a$  и  $2b$ , тоже делились бы на  $p$ , а потому на  $p$  делились бы также  $a$  и  $b$ , что противоречит предположению. Отсюда, наконец, вытекает, что среди чисел, которые не делятся на  $p$  и меньше модуля, имеется  $(p - 1)p^{n-1}/2$  вычетов, и что остальные числа, которых столько же, являются невычетами. Эту теорему можно было бы вывести также и по аналогии с п. 97 из рассмотрения индексов.

## 101

*Каждое не делящееся на  $p$  число, которое является вычетом для  $p$ , есть также вычет для  $p^n$ , а то число, которое есть невычет для  $p$ , будет также невычетом для  $p^n$ .*

Последняя часть этой теоремы очевидна. Поэтому, если бы первая часть была неверна, то среди чисел, которые меньше  $p^n$  и одновременно не делятся на  $p$ , вычетов для  $p$  было бы больше, чем для  $p^n$ , т. е. больше чем  $p^{n-1}(p - 1)/2$ . Но без труда видно, что среди указанных чисел количество вычетов числа  $p$  в точности равно  $p^{n-1}(p - 1)/2$ .

Точно так же легко найти квадрат, который сравним по модулю  $p^n$  с заданным вычетом, если известен квадрат, сравнимый с этим вычетом по модулю  $p$ .

Именно, если имеется некоторый квадрат  $a^2$ , который сравним с заданным вычетом  $A$  по модулю  $p^\mu$ , то квадрат, сравнимый с  $A$  по модулю  $p^\nu$  (где предполагается, что  $\nu > \mu$ , но  $\nu \leq 2\mu$ ), находится следующим образом. Мы полагаем основание искомого квадрата равным  $\pm a + xp^\mu$ , ибо именно такую форму оно, как легко видеть, и должно иметь. Тогда должно быть  $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv \equiv A \pmod{p^\nu}$  или, так как  $2\mu > \nu$ ,  $A - a^2 \equiv \pm 2axp^\mu \pmod{p^\nu}$ . Если

$A - a^2 = p^\mu d$ , то  $x$  есть значение выражения  $\pm d/2a \pmod{p^{\nu-\mu}}$ , которое эквивалентно выражению  $\pm (A - a^2)/2ap^\mu \pmod{p^\nu}$ .

Таким образом, если задан квадрат, который сравним с  $A$  по модулю  $p$ , то можно найти квадрат, который сравним с  $A$  по модулю  $p^2$ ; от него можно затем перейти к модулю  $p^4$ , затем к модулю  $p^8$  и т. д.

**Пример.** Если задан вычет 6, который сравним по модулю 5 с квадратом 1, то мы находим квадрат  $9^2$ , с которым он сравним по модулю 25, далее, квадрат  $16^2$ , с которым он сравним по модулю 125, и т. д.

## 102

Что же касается чисел, делящихся на  $p$ , то ясно, что их квадраты будут делиться на  $p^2$ , и потому все числа, делящиеся на  $p$ , но не делящиеся на  $p^2$ , являются невычетами числа  $p^n$ . Вообще же, если дано число  $p^k A$ , где  $A$  не делится на  $p$ , то нужно различать следующие случаи:

1. Если  $k \geq n$ , то  $p^k A \equiv 0 \pmod{p^n}$ , т. е. данное число есть вычет.

2. Если  $k < n$  и нечетно, то  $p^k A$  есть невычет.

Действительно, если бы было  $p^k A \equiv p^{2x+1} A \equiv s^2 \pmod{p^n}$ , то  $s^2$  делилось бы на  $p^{2x+1}$ , а это возможно только тогда, когда  $s$  делится на  $p^{x+1}$ . Но тогда  $s^2$  делилось бы также на  $p^{2x+2}$ , а потому (так как  $2x+2$ , очевидно, не больше  $n$ ), на это число делилось бы и  $p^{2x+1} A$ , т. е.  $A$  делилось бы на  $p$ , что противоречит предположению.

3. Пусть  $k$  меньше чем  $n$ , и четно. Тогда  $p^k A$  будет вычетом или невычетом по модулю  $p^n$  в зависимости от того, является ли  $A$  вычетом или невычетом по модулю  $p$ . Действительно, если  $A$  есть вычет по модулю  $p$ , то он будет вычетом и по модулю  $p^{n-k}$ . Но если  $A \equiv a^2 \pmod{p^{n-k}}$ , то  $Ap^k \equiv a^2 p^k \pmod{p^n}$  и  $a^2 p^k$  есть квадрат. Если же  $A$  невычет для  $p$ , то  $p^k A$  не может быть вычетом для  $p^n$ . В самом деле, если бы имело место  $p^k A \equiv a^2 \pmod{p^n}$ , то  $a^2$  обязательно должно было бы делиться на  $p^k$ . Частное было бы квадратом, сравнимым с  $A$  по модулю  $p^{n-k}$ , а потому также и по модулю  $p$ , т. е.  $A$  было бы квадратичным вычетом для  $p$ . Но это противоречит предположению.

Так как раньше мы исключили *случай*  $p = 2$ , сейчас мы должны кое-что сказать специально о нем. Если число 2 — модуль, то каждое число является вычетом; невычетов нет. Если модуль равен 4, то все нечетные числа вида  $4k + 1$  будут вычетами, а вида  $4k + 3$  — невычетами. Если, наконец, модуль равен 8 или более высокой степени числа 2, то все нечетные числа вида  $8k + 1$  будут вычетами, а все остальные, т. е. числа вида  $8k + 3$ ,  $8k + 5$ ,  $8k + 7$  — невычетами. Последняя часть этой теоремы следует из того, что квадрат всякого нечетного числа, будь оно вида  $4k + 1$  или  $4k - 1$ , имеет вид  $8k + 1$ . Первую же часть мы докажем следующим образом.

1. Если сумма или разность двух чисел делится на  $2^{n-1}$ , то квадраты этих чисел сравнимы по модулю  $2^n$ . Действительно, если одно из них равно  $a$ , то второе будет иметь вид  $2^{n-1}h \pm a$ , и для квадрата его имеем, что он  $\equiv a^2 \pmod{2^n}$ .

2. Каждое нечетное число, являющееся квадратичным вычетом по модулю  $2^n$ , сравнимо с квадратом некоторого числа, которое нечетно и меньше чем  $2^{n-2}$ . Именно, пусть  $a^2$  — квадрат, с которым сравнимо данное число, и  $a \equiv \pm \alpha \pmod{2^{n-1}}$ , где  $\alpha$  не превосходит половины модуля (п. 4); тогда  $a^2 \equiv \alpha^2$ . Тем самым и заданное число  $\equiv \alpha^2$ . Очевидно, что как  $a$ , так и  $\alpha$  нечетны, и  $\alpha < 2^{n-2}$ .

3. Квадраты всех нечетных чисел, меньших  $2^{n-2}$ , несравнимы по модулю  $2^n$ . В самом деле, пусть  $r$  и  $s$  — два таких числа. Если бы их квадраты были сравнимы по модулю  $2^n$ , то  $(r - s)(r + s)$  делилось бы на  $2^n$  (где предполагается  $r > s$ ). Но легко видеть, что числа  $r - s$  и  $r + s$  не могут одновременно делиться на 4, и потому, если одно из них делится на 2, то второе должно делиться на  $2^{n-1}$ , чтобы произведение делилось на  $2^n$ . Это, однако, невозможно, так как каждое из этих чисел меньше, чем  $2^{n-2}$ .

4. Наконец, если эти квадраты привести к их наименьшим положительным вычетам, то мы получим  $2^{n-3}$  различных квадратичных вычетов, которые меньше модуля\* и все имеют вид  $8k + 1$ . Но

---

\* Потому что количество нечетных чисел, меньших, чем  $2^{n-2}$ , равно  $2^{n-3}$ .

так как среди чисел, меньших модуля, имеется в точности  $2^{n-3}$  чисел вида  $8k + 1$ , то все они должны содержаться среди указанных вычетов. Это и нужно было доказать.

Чтобы найти квадрат, сравнимый с заданным числом вида  $8k + 1$  по модулю  $2^n$ , можно использовать метод, аналогичный методу из п. 101 (ср. также п. 88). Наконец, для четных чисел будет верным все то, что мы изложили в п. 102.

## 104

Относительно количества различных (т. е. несравнимых по модулю) значений, которые имеет выражение  $V \equiv \sqrt{A} \pmod{p^n}$ , когда  $A$  есть вычет по модулю  $p^n$ , из предыдущего легко можно вывести следующее. (Число  $p$  мы, как и раньше, предполагаем простым и для краткости сразу исключаем случай  $n = 1$ .)

I. Если  $A$  не делится на  $p$ , то  $V$  имеет одно значение для  $p = 2$ ,  $n = 1$ , именно  $V \equiv 1$ ; два значения, если  $p$  нечетно, а также, если  $p = 2$ ,  $n = 2$ ; именно, если одно из них мы обозначим через  $\equiv v$ , то другое будет  $\equiv -v$ ; четыре значения для  $p = 2$ ,  $n > 2$ ; именно, если одно из них  $\equiv v$ , то остальные суть  $\equiv -v$ ,  $2^{n-1} + v$ ,  $2^{n-1} - v$ .

II. Если же  $A$  делится на  $p$ , но не делится на  $p^n$ , то пусть наибольшая степень  $p$ , входящая в  $A$ , есть  $p^{2\mu}$  (очевидно, что ее показатель должен быть четным), и пусть  $A = ap^{2\mu}$ . Тогда ясно, что все значения  $V$  делятся на  $p^\mu$ , и все получающиеся после деления величины суть значения выражения  $V' = \sqrt{a} \pmod{p^{n-2\mu}}$ . Из них мы получим все различные значения  $V$ , если умножим на  $p^\mu$  все лежащие между 0 и  $p^{n-\mu}$  значения выражения  $V'$ . Поэтому значения  $V$  представляются в виде

$$vp^\mu, vp^\mu + p^{n-\mu}, vp^\mu + 2p^{n-\mu}, \dots, vp^\mu + (p^\mu - 1)p^{n-\mu},$$

где неизвестное  $v$  принимает все различные значения выражения  $V'$ , так что число значений  $V$  равно  $p^\mu$ ,  $2p^\mu$  или  $4p^\mu$  в зависимости от того, равно ли число значений  $V'$  (см. случай I) 1, 2 или 4.

III. Если  $A$  делится на  $p^n$ , то легко видеть, что если мы положим  $n = 2m$  или  $= 2m - 1$ , смотря по тому, четно  $n$  или нечетно, то значениями  $V$  будут все числа, делящиеся на  $p^m$ , и только они. Поэтому  $0, p^m, 2p^m, \dots, (p^{n-m} - 1)p^m$  дают все различные между собой значения, и число их равно  $p^{n-m}$ .

## 105

Остается случай, когда модуль составлен из нескольких различных простых чисел. Если  $m = abc \dots$ , где  $a, b, c, \dots$  обозначают или различные простые числа, или степени различных простых чисел, то прежде всего ясно, что если  $n$  есть вычет по модулю  $m$ , то оно будет вычетом и по всем модулям  $a, b, c, \dots$ , и потому  $n$ , очевидно, будет невычетом для  $m$ , если оно является невычетом хотя бы одного из чисел  $a, b, c, \dots$ . Но и наоборот, если  $n$  является вычетом всех чисел  $a, b, c, \dots$ , то оно будет и вычетом их произведения. Действительно, если мы положим  $n \equiv A^2, B^2, C^2, \dots$  соответственно по модулям  $a, b, c, \dots$ , то для числа  $N$ , полученного согласно п. 32, которое сравнимо с  $A, B, C, \dots$  соответственно по модулям  $a, b, c, \dots$ , будет иметь место  $n \equiv N^2$  по всем этим модулям, а потому также и по их произведению  $m$ . Так как легко видеть, что при комбинировании таким способом каждого значения числа  $A$  или выражения  $\sqrt{n} \pmod{a}$  с каждым значением числа  $B$ , с каждым значением числа  $C$  и т. д. получается значение числа  $N$ , т. е. выражения  $\sqrt{n} \pmod{m}$ , и, далее, из различных комбинаций получаются различные  $N$ , а из всевозможных комбинаций — всевозможные  $N$ , то количество всех различных значений  $N$  равно произведению количеств значений чисел  $A, B, C, \dots$ , определять которые мы научились в предыдущем пункте.

Далее, ясно, что если известно значение выражения  $\sqrt{n} \pmod{m}$  или  $N$ , то оно будет одновременно значением всех  $A, B, C, \dots$ , а так как, согласно предыдущему пункту, из него могут быть выведены все значения этих величин, то, следовательно, из одного значения  $N$  можно получить все остальные.

**Пример.** Пусть модуль равен 315, и спрашивается, является ли число 46 вычетом или невычетом. Простые делители числа 315

суть 3, 5, 7, и число 46 является вычетом по каждому из них, а потому и по модулю 315. Так как, далее,  $46 \equiv 1$  и  $\equiv 64$  по модулю 9,  $\equiv 1$  и  $\equiv 16$  по модулю 5,  $\equiv 4$  и  $\equiv 25$  по модулю 7, то основаниями квадратов, которые сравнимы с 46 по модулю 315, являются следующие числа: 19, 26, 44, 89, 226, 271, 289, 296.

**Общий критерий того, является ли заданное число вычетом или невычетом по заданному простому модулю**

### 106

Из предыдущего следует, что если только мы можем узнать, будет ли *заданное простое число* вычетом или невычетом по *заданному простому модулю*, то все остальные случаи могут быть сведены к этому. Поэтому мы должны направить наши усилия на то, чтобы получить точные критерии для решения первого вопроса. Однако, прежде чем приступить к этому исследованию, мы хотим указать на один критерий, получающийся на основании предыдущего раздела, который хотя и не находит себе почти никогда применения на практике, но все же достоин упоминания вследствие своей простоты и общности.

*Каждое число  $A$ , которое не делится на простое число  $2m + 1$ , является вычетом или невычетом по этому простому числу, в зависимости от того, имеет ли место  $A^m \equiv +1$  или  $\equiv -1 \pmod{2m + 1}$ .*

Именно, если для модуля  $2m + 1$  индекс числа  $A$  в некоторой системе равен  $a$ , то  $a$  будет четным, если  $A$  есть вычет числа  $2m + 1$ , и нечетным, если  $A$  — невычет. Индекс же числа  $A^m$  равен  $ma$ , т. е. он  $\equiv 0$  или  $\equiv m \pmod{2m}$ , смотря по тому, четно  $a$ , или нечетно. Отсюда вытекает, что в первом случае  $A^m \equiv +1$ , а во втором случае  $A^m \equiv -1 \pmod{2m + 1}$ . (ср. пп. 57 и 62).

**Пример.** 3 есть вычет числа 13, потому что  $3^6 \equiv 1 \pmod{13}$ ; наоборот, 2 — невычет по модулю 13, ибо  $2^6 \equiv -1 \pmod{13}$ .

Однако, если исследуемые числа более или менее большие, этот критерий становится полностью непригодным вследствие громоздкости вычислений.



## Исследования относительно простых чисел, по которым заданные числа являются вычетами или невычетами

107

Итак, для заданного модуля совсем легко указать все те числа, которые являются для него вычетами или невычетами. Действительно, если заданный модуль  $= m$ , то нужно только найти квадраты чисел, не превосходящих половины  $m$ , или даже только числа, сравнимые по модулю  $m$  с этими квадратами (практически существуют еще более удобные методы), и тогда все числа, сравнимые с каким-нибудь из полученных чисел по модулю  $m$ , будут вычетами, а все числа, не сравнимые ни с одним из них, — невычетами. Однако обратная задача: *если задано некоторое число, определить все те числа, по которым оно является вычетом или невычетом*, — значительно сложнее. Этой задачей, от решения которой зависит и решение проблемы, поставленной в предыдущем разделе, мы будем теперь заниматься и начнем при этом с простейших случаев.

### Вычет—1

108

**Теорема.** *Число —1 является квадратичным вычетом по всем простым числам вида  $4n + 1$  и невычетом по всем простым числам вида  $4n + 3$ .*

**Пример.** —1 является вычетом чисел 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, ... и сравнимо соответственно с квадратами чисел 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, ...; и напротив, —1 является невычетом чисел 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, ...

Мы уже упоминали об этой теореме в п. 64. Доказательство же легко получается из п. 106. Действительно, для простого числа вида  $4n + 1$  имеет место  $(-1)^{2n} \equiv 1$ , а для простого числа вида  $4n + 3$  будет  $(-1)^{2n-1} \equiv -1$ . Это доказательство совпадает с доказательством, приведенным в вышеупомянутом месте. Однако вследствие красоты и полезности теоремы не будет лишним доказать ее еще другим способом.

Совокупность всех вычетов простого числа  $p$ , меньших  $p$ , за исключением вычета 0, мы обозначим буквой  $C$ . Так как число этих вычетов всегда равно  $(p - 1)/2$ , оно, очевидно, будет четным, если  $p$  имеет вид  $4n + 1$ , и нечетным, если  $p$  имеет вид  $4n + 3$ . Аналогично п. 77, где речь шла о любых числах, мы будем называть ассоциированными *те вычеты, произведение которых  $\equiv 1 \pmod{p}$* ; действительно, если  $r$  есть вычет, то и  $1/r$ , очевидно, будет вычетом по модулю  $p$ . Так как один и тот же вычет не может иметь в  $C$  других ассоциированных вычетов, ясно, что все вычеты из  $C$  могут быть разбиты на классы, каждый из которых содержит два ассоциированных вычета. Далее, ясно, что если нет вычетов, ассоциированных с самими собой, т. е. если каждый класс содержит два неравных вычета, то число всех вычетов должно быть равно удвоенному числу всех классов. Если же имеются вычеты, ассоциированные сами с собой, т. е. если имеются классы, содержащие только один вычет, или, если такое выражение больше нравится, содержащие этот один вычет дважды, то, полагая число таких классов равным  $a$ , а число остальных классов равным  $b$ , мы получим, что число всех вычетов в  $C$  равно  $a + 2b$ . Поэтому, если  $p$  имеет вид  $4n + 1$ , то  $a$  четно; если же  $p$  имеет вид  $4n + 3$ , то  $a$  нечетно. Но среди чисел, меньших  $p$ , никакие, кроме 1 и  $p - 1$ , не могут быть ассоциированы сами с собой (ср. п. 77), а 1, очевидно, всегда есть вычет. Поэтому  $p - 1$  (или, что то же самое,  $-1$ ) в первом случае должно быть вычетом, а во втором невычетом, ибо иначе в первом случае имело бы место  $a = 1$ , а во втором  $a = 2$ , что невозможно.

Этим доказательством мы также обязаны Э й л е р у, который дал и первое доказательство этой теоремы вообще (ср. «*Opusc. Analyt.*», Т. I, р. 135). Легко заметить, что оно базируется на принципах, подобных тем, на которых основано наше второе доказательство теоремы В и л ь с о н а в п. 77. Если же опираться на эту теорему, то доказательство можно провести еще проще. Среди чисел 1, 2,

3, ...,  $p - 1$  имеется  $(p - 1)/2$  квадратичных вычетов по модулю  $p$  и столько же невычетов. Поэтому количество невычетов четно, если  $p$  имеет вид  $4n + 1$ , и нечетно, если  $p$  имеет вид  $4n + 3$ . Таким образом, произведение всех чисел  $1, 2, 3, \dots, p - 1$  в первом случае является вычетом, а во втором — невычетом (п. 99). Но это произведение всегда  $\equiv -1 \pmod{p}$ ; следовательно,  $-1$  в первом случае есть вычет, а во втором — невычет.

## 111

Из сказанного следует, что если  $r$  есть вычет простого числа вида  $4n + 1$ , то и  $-r$  будет вычетом этого простого числа, и наоборот, все невычеты такого числа, взятые с отрицательным знаком, остаются невычетами \*. Обратное имеет место в случае простых чисел вида  $4n + 3$ , вычеты которых при перемене знака превращаются в невычеты, и наоборот. (Ср. п. 98.)

Наконец, из всего сказанного легко получается следующее общее правило:  $-1$  является вычетом всех чисел, которые не делятся ни на 4, ни на какое-либо простое число вида  $4n + 3$ , и невычетом всех остальных чисел (ср. пп. 103 и 105).

Вычеты  $+2$  и  $-2$ 

## 112

Теперь мы переходим к вычетам  $+2$  и  $-2$ .

Если мы соберем в таблице 2 все простые числа, для которых  $+2$  является вычетом, то получим следующие: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Легко заметить, что среди них нет чисел вида  $8n + 3$  и  $8n + 5$ . Поэтому мы должны постараться строго обосновать это индуктивное заключение.

Прежде всего, заметим, что каждое составное число вида  $8n + 3$  или  $8n + 5$  обязательно содержит простой сомножитель одного из этих видов; действительно, только из простых чисел вида  $8n + 1$  и

---

\* Таким образом, если мы говорим о некотором числе как о вычете или невычете числа вида  $4n + 1$ , то мы можем просто отбрасывать знак рассматриваемого числа или же снабжать его двойным знаком  $\pm$ .

$8n + 7$ , очевидно, не могут быть составлены другие числа, кроме имеющих вид  $8n + 1$  и  $8n + 7$ . Поэтому, если наше индуктивное заключение правильно, то вообще не должно быть чисел вида  $8n + 3$  или  $8n + 5$ , для которых  $+2$  было бы вычетом. Как легко проверить, среди чисел до 100 действительно нет чисел указанного вида, для которых  $+2$  было бы вычетом. Если же мы предположим, что по другую сторону этой границы такие числа есть, то пусть наименьшее из них равно  $t$ ; таким образом,  $t$  имеет вид или  $8n + 3$ , или  $8n + 5$ , и  $+2$  является для него вычетом, в то время как для всех меньших чисел такого вида — невычетом. Если положить  $2 \equiv a^2 \pmod{t}$ , то всегда можно считать, что  $a$  нечетно и меньше  $t$  (действительно,  $a$  обладает по меньшей мере двумя положительными значениями, меньшими  $t$ , сумма которых равна  $t$ , и из которых поэтому одно четно, а другое нечетно (ср. пп. 104 и 105)). Если же это условие выполнено, и  $a^2 = 2 + tu$ , или  $tu = a^2 - 2$ , то  $a^2$  будет иметь вид  $8n + 1$ , и  $tu$ , таким образом, — вид  $8n - 1$ , и потому  $u$  будет или вида  $8n + 3$ , или вида  $8n + 5$ , в зависимости от того, имеет ли  $t$  второй или первый из этих видов. Из равенства  $a^2 = 2 + tu$  следует, что  $2 \equiv a^2 \pmod{u}$ , т. е. 2 является также вычетом числа  $u$ . Но легко видеть, что  $u < t$ , и потому  $t$ , вопреки нашему предположению, не является наименьшим среди чисел, для которых наше индуктивное заключение неверно. Отсюда, очевидно, следует, что то, что мы установили индуктивным путем, действительно всегда справедливо.

Если мы скомбинируем это с теоремами, найденными в п. 111, то получим следующие теоремы.

I. Для всех простых чисел вида  $8n + 3$  число  $+2$  есть невычет, а  $-2$  — вычет.

II. Для всех простых чисел вида  $8n + 5$  как  $+2$ , так и  $-2$  являются невычетами.

### 113

Аналогичным образом из таблицы 2 мы находим \* следующие простые числа, для которых  $-2$  является квадратичным вычетом: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97. Так как среди них нет

\* Рассматривая  $-2$  как произведение чисел  $+2$  и  $-1$  (ср. п. 111).

чисел вида  $8n + 5$  и  $8n + 7$ , исследуем, справедливо ли это индуктивное заключение вообще. Подобно тому, как в предыдущем можно показать, что каждое составное число вида  $8n + 5$  или  $8n + 7$  содержит простой сомножитель вида  $8n + 5$  или  $8n + 7$ , так что, если наше индуктивное заключение вообще справедливо, то  $-2$  не может быть вычетом никаких чисел вида  $8n + 5$  или  $8n + 7$ . Если же предположить, что такие числа существуют, то пусть наименьшее из них равно  $t$ , и  $-2 = a^2 - tu$ . При этом, если, как и выше, предположить, что  $a$  нечетно и меньше, чем  $t$ , то  $u$  будет иметь вид  $8n + 5$  или  $8n + 7$ , в зависимости от того, имеет ли  $t$  вид  $8n + 7$  или  $8n + 5$ . Но из того, что  $a^2 + 2 = tu$  и  $a < t$ , легко вывести, что  $u$  тоже меньше  $t$ . Наконец,  $-2$  будет также и вычетом числа  $u$ , т. е.  $t$ , в противоречие с предположением, не является наименьшим числом, для которого наше индуктивное заключение неверно. Итак,  $-2$  обязательно является невычетом всех чисел вида  $8n + 5$  и  $8n + 7$ .

Если связать это с теоремой п. 111, то получаются следующие теоремы.

I. Для всех простых чисел вида  $8n + 5$  как  $-2$ , так и  $+2$  являются невычетами, что мы уже доказали в предыдущем пункте.

II. Для всех простых чисел вида  $8n + 7$  число  $-2$  является невычетом, а  $+2$  — вычетом.

Впрочем, в каждом из двух доказательств мы могли брать для  $a$  также и четное значение; тогда мы должны были бы различать случаи, когда  $a$  имеет вид  $4n + 2$  или  $4n$ . Рассуждения протекают точно так же, как и выше, и не вызывают никаких трудностей.

#### 114

Остается еще один случай, а именно тот, когда простое число имеет вид  $8n + 1$ . Но для него прежние методы оказываются непригодными, а нужен специальный искусственный прием.

Если для модуля, являющегося простым числом вида  $8n + 1$ , некоторый первообразный корень равен  $a$ , то (п. 62)  $a^{4n} \equiv -1 \pmod{8n+1}$ , а это сравнение может быть также представлено в виде  $(a^{2n} + 1)^2 \equiv \equiv 2a^{2n} \pmod{8n+1}$ , или в виде  $(a^{2n} - 1)^2 \equiv -2a^{2n}$ . Отсюда следует,

что как  $2a^{2n}$ , так и  $-2a^{2n}$  являются вычетами по модулю  $8n + 1$ . Но так как  $a^{2n}$  есть не делящийся на модуль квадрат, то, очевидно,  $+2$  и  $-2$  суть вычеты (п. 98)\*.

## 115

Не будет бесполезным добавить и *другое доказательство этой теоремы*, которое относится к предыдущему так же, как второе доказательство (п. 109) теоремы из п. 108 — к первому (п. 108). Разбирающиеся в этих вопросах тогда легче поймут, что и в том, и в другом случае оба доказательства не настолько отличаются одно от другого, как это может показаться на первый взгляд.

I. Для любого простого модуля вида  $4m + 1$  среди чисел  $1, 2, 3, \dots, 4m$ , которые меньше модуля, имеется  $m$  чисел, сравнимых с биквадратами, а остальные  $3m$  — с биквадратами не сравнимы.

Хотя это легко можно вывести из соображений предыдущего раздела, но и без этого доказательство не сложно. Именно, мы уже доказали, что для такого модуля  $-1$  всегда есть квадратичный вычет. Если, таким образом,  $f^2 \equiv -1$ , то для любого не делящегося на модуль числа  $z$  биквадраты четырех чисел  $+z, -z, +fz, -fz$  (которые, как легко видеть, не сравнимы один с другим) будут сравнимы между собой. Далее, ясно, что биквадрат какого-нибудь числа, не сравнимого ни с одним из этих четырех чисел, не может быть сравним с их биквадратом (действительно, в противном случае сравнение четвертой степени  $x^4 \equiv z^4$ , в противоречие с п. 43, имело бы более четырех корней). Отсюда легко следует, что числа  $1, 2, 3, \dots, 4m$  порождают только  $m$  не сравнимых биквадратов, с которыми среди этих чисел имеется  $m$  сравнимых, в то время как остальные не могут быть сравнимыми с биквадратами.

II. По простому модулю вида  $8n + 1$  число  $-1$  сравнимо с некоторым биквадратом ( $-1$  является биквадратичным *вычетом* этого простого числа).

---

\* Короче доказательство проводится так: имеет место  $(a^{3n} - a^n)^2 = 2 + (a^{4n} + 1)(a^{2n} - 2)$  и  $(a^{3n} + a^n)^2 = -2 + (a^{4n} + 1)(a^{2n} + 2)$ . Поэтому  $\sqrt{2} \equiv \pm (a^{3n} - a^n)$  и  $\sqrt{-2} \equiv \pm (a^{3n} + a^n) \pmod{8n + 1}$

Именно, число всех биквадратичных вычетов, меньших, чем  $8n + 1$  (за исключением нуля), равно  $2n$ , т. е. четно. Далее, легко показать, что если  $r$  есть биквадратичный вычет числа  $8n + 1$ , то таковым будет и значение выражения  $\frac{1}{r} \pmod{8n + 1}$ . Поэтому все биквадратичные вычеты могут быть разбиты на классы, подобно тому, как мы это сделали в п. 109 для квадратичных вычетов. Остальная часть доказательства может быть теперь проведена совершенно тем же способом, как и там.

III. Пусть теперь  $g^4 \equiv -1$ , и  $h$  есть значение выражения  $\frac{1}{g} \pmod{8n + 1}$ . Тогда (так как  $gh \equiv 1$ )

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2.$$

Но  $g^4 \equiv -1$ , откуда  $-h^2 \equiv g^4 h^2 \equiv g^2$ , т. е.  $g^2 + h^2 \equiv 0$  и  $(g \pm h)^2 \equiv \pm 2$ , и потому как  $+2$ , так и  $-2$  являются квадратичными вычетами по модулю  $8n + 1$ .

## 116

Наконец, из предыдущего легко выводится следующее **общее правило**:

$+2$  является вычетом каждого числа, которое не делится на 4 и на любое простое число вида  $8n + 3$  или  $8n + 5$ , и невычетом всех остальных (например, всех чисел вида  $8n + 3$  или  $8n + 5$ , будь они простыми или составными).

$-2$  является вычетом каждого числа, которое не делится на 4 и на любое простое число вида  $8n + 5$  или  $8n + 7$ , и невычетом всех остальных.

Эти изящные теоремы были уже известны проницательному Ферма, «*Op. Mathem.*», р. 168. Однако он нигде не сообщил доказательства, о котором утверждал, что оно у него имеется. Позже доказательство все время безуспешно искал Эйлер; впервые строгое доказательство дал Лагранж («*Nouv. Mém. de l'Acad. de Berlin*», 1775, р. 349, 351). Оно, по-видимому, не было известно Эйлеру, когда он опубликовал свою работу, помещенную в «*Opusc. Analyt.*», Т. I, р. 259.

Вычеты  $+3$  и  $-3$ 

117

Теперь мы переходим к вычетам  $+3$  и  $-3$ , причем начинаем со второго.

Из таблицы 2 мы находим следующие простые числа, для которых  $-3$  является вычетом: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97. Среди них нет ни одного числа вида  $6n + 5$ . А то, что и за пределами границы таблицы нет простых чисел такого вида, для которых  $-3$  является вычетом, мы докажем следующим образом. Прежде всего, ясно, что каждое составное число вида  $6n + 5$  обязательно содержит простой сомножитель такого же вида. Поэтому до той границы, до которой нет простых чисел вида  $6n + 5$ , имеющих  $-3$  вычетом, нет также и составных чисел того же вида с тем же свойством. Если предположить, что за пределами нашей таблицы такие числа существуют, то пусть наименьшее из них равно  $t$  и  $-3 = a^2 - tu$ . Тогда, если считать, что  $a$  взято четным и меньшим чем  $t$ , будет иметь место  $u < t$  и  $-3$  будет вычетом для  $u$ . Но если  $a$  имеет вид  $6n \pm 2$ , то  $tu$  будет иметь вид  $6n + 1$ , и потому  $u$  — вид  $6n + 5$ . Это, однако, невозможно, так как по нашему предположению  $t$  есть наименьшее число, для которого наше индуктивное предположение неверно. Если же  $a$  имеет вид  $6n$ , то  $tu$  будет иметь вид  $36n + 3$  и потому  $tu/3$  — вид  $12n + 1$ , а  $u/3$  — вид  $6n + 5$ . Но ясно, что  $-3$  является вычетом для  $u/3$  и  $\frac{u}{3} < t$ . Это, однако, невозможно. Поэтому ясно, что  $-3$  не может быть вычетом никакого числа вида  $6n + 5$ .

Так как каждое число вида  $6n + 5$  представляется обязательно или в виде  $12n + 5$ , или в виде  $12n + 11$ , а потому в первом случае может быть также записано в виде  $4n + 1$ , а во втором — в виде  $4n + 3$ , мы имеем следующие теоремы.

I. Для каждого простого числа вида  $12n + 5$  как  $-3$ , так и  $+3$  являются невычетами.

II. Для каждого простого числа вида  $12n + 11$  число  $-3$  является невычетом, а число  $+3$  — вычетом.



## 118

В качестве чисел, имеющих  $+3$  вычетом, в таблице 2 находятся следующие: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97; среди них нет ни одного числа вида  $12n + 5$  или  $12n + 7$ . То, что вообще нет чисел вида  $12n + 5$ ,  $12n + 7$ , для которых  $+3$  является вычетом, может быть доказано точно таким же образом, как в пп. 112, 113, 117, и потому мы не будем на этом останавливаться. В соединении с п. 111 мы получаем следующие теоремы.

I. Для каждого простого числа вида  $12n + 5$  как  $+3$ , так и  $-3$  являются невычетами (что мы нашли уже в предыдущем пункте).

II. Для каждого простого числа вида  $12n + 7$  число  $+3$  является невычетом, а число  $-3$  — вычетом.

## 119

Таким путем, однако, ничего нельзя узнать относительно чисел вида  $12n + 1$ , которые поэтому требуют для своего рассмотрения специальных приемов. Правда, индуктивным способом легко установить, что  $+3$  и  $-3$  являются вычетами всех простых чисел такого вида. Кроме того, очевидно, нужно только доказать, что  $-3$  является вычетом всех таких чисел, потому что тогда и  $+3$  обязательно будет вычетом (п. 111). Мы, однако, докажем более общий факт, а именно, что  $-3$  есть вычет каждого простого числа вида  $3n + 1$ .

Пусть  $p$  — такое простое число, и  $a$  — число, принадлежащее по модулю  $p$  показателю 3 (то, что такое число существует, вытекает из п. 54, так как 3 есть делитель числа  $p - 1$ ). Тогда  $a^3 \equiv 1 \pmod{p}$ , т. е.  $a^3 - 1$  или  $(a^2 + a + 1)(a - 1)$  делится на  $p$ . Однако, очевидно, что не может быть  $a \equiv 1 \pmod{p}$ , так как 1 принадлежит показателю 1, и потому не  $a - 1$ , а обязательно  $a^2 + a + 1$  делится на  $p$ , а, следовательно, делится и  $4a^2 + 4a + 4$ , т. е.  $(2a + 1)^2 \equiv -3 \pmod{p}$ , и значит  $-3$  есть вычет по модулю  $p$ .

Между прочим ясно, что это доказательство (которое не опирается на изложенное выше) охватывает также и простые числа вида  $12n + 7$ , которые мы уже рассмотрели в предыдущем пункте.

Можно еще заметить, что это исследование может быть проведено также методами, аналогичными тем, что применялись в пп. 109, 115, но ради краткости мы не будем в это вдаваться.

Из предыдущего легко получаются следующие теоремы (ср. пп. 102, 103, 105).

I.—3 является вычетом всех чисел, которые не делятся ни на 8, ни на 9 и ни на какое простое число вида  $6n + 5$ , и невычетом всех остальных чисел.

II.  $+3$  является вычетом всех чисел, которые не делятся ни на 4, ни на 9, ни на какое простое число вида  $12n + 5$  или  $12n + 7$ , и невычетом всех остальных чисел.

Специально можно отметить следующий частный случай.

— 3 является вычетом всех простых чисел вида  $3n + 1$ , или, что то же самое, всех простых чисел, которые являются вычетами числа 3, и является невычетом всех простых чисел вида  $6n + 5$ , или, за исключением числа 2, всех простых чисел вида  $3n + 2$ , т. е. всех, которые являются невычетами числа 3. Легко убедиться, что все остальные случаи вытекают отсюда.

Теоремы, касающиеся вычетов  $+3$  и  $-3$ , были уже известны Ф е р м а, «*Opera Wallisii*», Т. II, р. 857, хотя доказательства впервые дал Э й л е р, «*Comm Nov. Petr.*», Т. VIII, р. 105 и сл. Поэтому особенно удивительно, что доказательства теорем относительно вычетов  $+2$  и  $-2$ , которые основываются на подобных же принципах, не поддались его усилиям (ср. также сочинение Ла г р а н ж а, «*Nouv. Mém. de l'Ac. de Berlin*», р. 352).

## Вычеты $+5$ и $-5$

Индуктивным путем мы находим, что  $+5$  не является вычетом никакого нечетного числа вида  $5n + 2$  или  $5n + 3$ , т. е. никакого нечетного числа, которое есть невычет числа 5. То, что это правило не имеет исключений, доказывается так. Пусть наименьшее число, составляющее исключение из этого правила, если такие вообще существуют, равно  $t$ , так что оно есть невычет числа 5, в то время как 5 является его вычетом. Пусть, далее,  $a^2 = 5 + tu$ , где  $a$  четно и меньше, чем  $t$ . Тогда  $u$  будет нечетным и меньшим, чем  $t$ , а  $+5$  будет вычетом по модулю  $u$ . Если теперь  $a$  не делится на 5, то это будет

иметь место и для  $u$ ; но очевидно, что  $tu$  есть вычет числа 5, а так как  $t$  является невычетом по модулю 5, то  $u$  тоже будет невычетом. Таким образом, существует нечетный невычет числа 5, для которого  $+5$  является вычетом, и которое меньше, чем  $t$ . Но это находится в противоречии с нашим предположением. Если же  $a$  делится на 5, то полагая  $a = 5b$  и  $u = 5v$ , мы получим  $tv \equiv -1 \equiv 4 \pmod{5}$ , т. е.  $tv$  будет вычетом числа 5. Далее доказательство проводится точно так же, как и в первом случае.

## 122

*Итак, для всех простых чисел, которые одновременно являются невычетами числа 5 и имеют вид  $4n + 1$ , т. е. для всех простых чисел вида  $20n + 13$  или  $20n + 17$  числа  $+5$  и  $-5$  являются невычетами; для всех же простых чисел вида  $20n + 3$  или  $20n + 7$  число  $+5$  есть невычет, а  $-5$  — вычет.*

Совершенно аналогичным способом можно показать, что  $-5$  является невычетом всех простых чисел вида  $20n + 11$ ,  $20n + 13$ ,  $20n + 17$ ,  $20n + 19$ , а отсюда, как легко видеть, следует, что  $+5$  есть вычет всех простых чисел вида  $20n + 11$  или  $20n + 19$  и невычет всех простых чисел вида  $20n + 13$  или  $20n + 17$ . И так как каждое простое число, кроме 2 и 5 (для которых  $\pm 5$  есть вычет), представляется в одном из видов  $20n + 1, 3, 7, 9, 11, 13, 17, 19$ , то мы, очевидно, уже можем решить наш вопрос относительно всех простых чисел, кроме тех, которые имеют вид  $20n + 1$  или  $20n + 9$ .

## 123

Индуктивным путем легко находится, что  $+5$  и  $-5$  являются вычетами всех простых чисел вида  $20n + 1$  или  $20n + 9$ . Если бы это было верно вообще, мы имели бы изящную теорему, именно, что  $+5$  есть вычет всех простых чисел, которые являются вычетами числа 5 (так как эти последние представляются в одном из видов  $5n + 1$  или  $5n + 4$ , т. е. в одном из видов  $20n + 1, 9, 11, 19$ , а для третьего и четвертого из этих видов этот факт уже доказан), и невычетом всех нечетных простых чисел, которые являются невычетами числа 5,

что мы уже доказали выше. Ясно, что этой теоремы достаточно, чтобы уметь решать, является ли  $+5$  (а тем самым и  $-5$ , если рассматривать его как произведение  $+5$  и  $-1$ ) вычетом или невычетом любого заданного числа. Наконец, можно было бы отметить аналогичность этой теоремы той, которую мы вывели в п. 120 относительно вычета  $-3$ .

Однако доказать это индуктивное заключение не очень легко. Если задано некоторое простое число вида  $20n + 1$  или, более общо, вида  $5n + 1$ , то с вопросом можно покончить подобным же образом, как в пп. 114, 119. Именно, если  $a$  — какое-нибудь число, принадлежащее по модулю  $5n + 1$  показателю 5 (то, что такое существует, вытекает из предыдущего раздела), то  $a^5 \equiv 1$ , или  $(a - 1)(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{5n + 1}$ . Но так как не может быть  $a \equiv 1$ , т. е.  $a - 1 \equiv 0$ , то обязательно  $a^4 + a^3 + a^2 + a + 1 \equiv 0$ . Поэтому также  $4(a^4 + a^3 + a^2 + a + 1) = (2a^2 + a + 2)^2 - 5a^2 \equiv 0$ , т. е.  $5a^2$  есть вычет числа  $5n + 1$ , а значит и 5 — вычет этого числа, потому что  $a^2$  есть вычет, не делящийся на  $5n + 1$  (действительно,  $a$  не делится на  $5n + 1$  вследствие того, что  $a^5 \equiv 1$ ).

Случай же, когда дано простое число вида  $5n + 4$ , требует более глубоких вспомогательных средств. Но так как теоремы, при помощи которых решается этот вопрос, в дальнейшем будут изложены в более общем виде, мы коснемся их здесь лишь коротко.

I. Если  $p$  — простое число, и  $b$  — его заданный квадратичный невычет, то значение выражения

$$A = \frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$$

(в котором при раскрытии скобок, как легко видеть, иррациональность пропадает) делится на  $p$  при любом  $x$ , в том числе и при  $x = p$ . Именно, при первом взгляде на коэффициенты, которые получаются при разложении  $A$ , видно, что все члены от второго до предпоследнего включительно делятся на  $p$ , и потому

$$A \equiv 2(p + 1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}.$$

Но так как  $b$  есть невычет по модулю  $p$ , то  $b^{(p-1)/2} \equiv -1 \pmod{p}$  (п. 106); в то же время  $x^p$  всегда  $\equiv x$  (согласно предыдущему разделу); поэтому  $A \equiv 0$ .

II. Сравнение  $A \equiv 0 \pmod{p}$  имеет относительно  $x$  степень  $p$ , и все числа  $0, 1, 2, \dots, p-1$  являются его корнями. Если теперь  $e$  есть делитель числа  $p+1$ , то выражение

$$\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$$

(которое мы обозначим через  $B$ ) после раскрытия скобок будет свободно от иррациональности, относительно  $x$  будет иметь степень  $e-1$ , и, как известно из первых элементов анализа,  $A$  будет (как многочлен) делиться на  $B$ . Теперь я утверждаю, что имеется  $e-1$  значений  $x$ , которые будучи подставлены в  $B$ , делают  $B$  делящимся на  $p$ . Именно, если положить  $A \equiv BC$ , то  $C$  будет иметь относительно  $x$  степень  $p-e+1$ , и потому сравнение  $C \equiv 0 \pmod{p}$  обладает не более чем  $p-e+1$  корнями. Отсюда легко следует, что все остальные  $e-1$  чисел из ряда  $0, 1, 2, 3, \dots, p-1$  являются корнями сравнения  $B \equiv 0$ .

III. Предположим теперь, что  $p$  имеет вид  $5n+4$ ,  $e=5$ ,  $b$  — нечет по модулю  $p$ , и число  $a$  определено так, что выражение

$$\frac{(a + \sqrt{b})^5 - (a - \sqrt{b})^5}{\sqrt{b}}$$

делится на  $p$ . Но это выражение равно

$$10a^4 + 20a^2b + 2b^2 = 2[(b + 5a^2)^2 - 20a^4],$$

и потому также  $(b + 5a^2)^2 - 20a^4$  делится на  $p$ , т. е.  $20a^4$  есть вычет по модулю  $p$ . Так как, однако,  $4a^4$  есть вычет, не делящийся на  $p$  (действительно, легко видеть, что  $a$  не делится на  $p$ ), то также и  $5$  будет вычетом по модулю  $p$ , что и требовалось доказать.

Отсюда следует, что указанная в начале этого пункта теорема вообще верна.

Заметим еще, что доказательством для обоих случаев мы обязаны Лагранжу, «*Mém. de l'Ac. de Berlin*», 1775, p. 352 и сл.

О вычетах  $\pm 7$ 

124

Подобным же образом доказывается, что  $-7$  есть невычет каждого числа, которое является невычетом числа 7.

По индукции же можно заключить, что  $-7$  есть вычет каждого числа, которое является вычетом числа 7.

Однако до сих пор это никем не было строго доказано. Впрочем, для тех вычетов числа 7, которые имеют вид  $4n - 1$ , доказательство просто. Действительно, уже достаточно хорошо известным из предыдущего путем можно показать, что  $+7$  всегда невычет, а потому  $-7$  — вычет таких простых чисел. Но это дает слишком мало, так как остальные случаи этому методу не поддаются. Лишь еще один случай можно исследовать способом, подобным использованному в пп. 119 и 123. Именно, если  $p$  есть простое число вида  $7n + 1$ , и  $a$  — число, принадлежащее по модулю  $p$  показателю 7, то легко видеть, что выражение

$$\frac{4(a^7 - 1)}{a - 1} = (2a^3 + a^2 - a - 2)^2 + 7(a^2 + a)^2$$

всегда делится на  $p$ , и потому  $-7(a^2 + a)^2$  есть вычет по модулю  $p$ . Но  $(a^2 + a)^2$ , будучи квадратом, является вычетом числа  $p$  и притом не делится на  $p$ ; действительно, так как  $a$  по предположению принадлежит показателю 7, оно не может быть ни  $\equiv 0$ , ни  $\equiv 1 \pmod{p}$ , т. е. на  $p$  не делятся ни  $a$ , ни  $a + 1$ , а потому и квадрат  $(a + 1)^2 a^2$ . Таким образом, также и 7 является, очевидно, вычетом числа  $p$ , что и нужно было доказать. Впрочем, и это доказательство впервые было найдено Л а г р а н ж е м в сочинении, упомянутом в конце п. 123. Ниже, в разделе VII, мы докажем, что вообще выражение  $4(x^p - 1)/(x - 1)$  всегда может быть приведено к виду  $X^2 \pm pY^2$  (верхний знак нужно брать, когда  $p$  — простое число вида  $4n + 1$ , а нижний — когда оно простое число вида  $4n + 3$ ), где  $X$  и  $Y$  суть целые рациональные функции от  $x$ . Л а г р а н ж для значений  $p$ , превышающих 7, этого разложения не провел (ср. указанное в п. 123 сочинение, стр. 352).

## Подготовка к общему исследованию

125

Так как применявшиеся до сих пор методы оказываются недостаточными для проведения общего доказательства, пора изложить другой метод, у которого этого недостатка нет. Мы начнем с теоремы, которая долго не поддавалась нашим усилиям доказать ее, хотя справедливость ее с первого взгляда кажется настолько очевидной, что некоторые даже не признавали необходимости ее доказательства. Эта теорема состоит в следующем. *Любое число, за исключением положительных квадратов, является невычетом некоторого простого числа.* Так как, однако, мы будем пользоваться этой теоремой только как вспомогательным средством для доказательства других предложений, мы разберем только те случаи, которые будут нужны для этой цели. Справедливость остальных случаев позднее получится сама собой. Сейчас мы докажем, что *каждое простое число вида  $4n + 1$ , взятое как положительным, так и отрицательным\**, является невычетом какого-нибудь простого числа, и притом (если заданное число  $> 5$ ) такого, которое меньше, чем оно само.

Если сначала задано простое число  $p$  вида  $4n + 1$ , которое нужно брать *отрицательным* (мы будем считать, что  $p > 17$ ;  $-13$  является невычетом числа 3, а  $-17$  — невычетом числа 5), то пусть  $2a$  — первое четное число, большее, чем  $\sqrt{p}$ ; тогда легко видеть, что  $4a^2 < 2p$  или  $4a^2 - p < p$ . Но  $4a^2 - p$  имеет вид  $4n + 3$ , а  $+p$  есть квадратичный вычет числа  $4a^2 - p$  (так как  $p \equiv 4a^2 \pmod{4a^2 - p}$ ). Поэтому, если  $4a^2 - p$  есть простое число, то  $-p$  будет его невычетом; если же оно не простое, то хотя бы один из его простых сомножителей обязательно имеет вид  $4n + 3$ , и так как  $+p$  есть вычет также и этого сомножителя,  $-p$  будет его невычетом.

Относительно простых чисел, которые должны браться *положительными*, мы будем различать два случая. Пусть сначала  $p$  — простое число вида  $8n + 5$ . Если  $a$  есть любое положительное число, которое  $< \sqrt{p/2}$ , то  $8n + 5 - 2a^2$  будет положительным числом вида  $8n + 5$  или  $8n + 3$  (в зависимости от того, четно  $a$  или не-

---

\* Разумеется, число  $+1$  должно быть исключено.

четно) и потому обязательно будет делиться на какое-нибудь простое число вида  $8n + 3$  или  $8n + 5$ , ибо произведение любого количества чисел вида  $8n + 1$  и  $8n + 7$  не может иметь ни вида  $8n + 3$ , ни вида  $8n + 5$ . Если указанное простое число равно  $q$ , то  $8n + 5 \equiv 2a^2 \pmod{q}$ . Но 2 является невычетом числа  $q$  (п. 112), а потому невычетами будут также  $2a^2$  и  $8n + 5$  \*.

## 126

Однако то, что каждое простое число вида  $8n + 1$ , взятое положительным, является невычетом какого-нибудь простого числа, меньшего, чем оно само, уже не может быть доказано такими простыми средствами. Но так как эта истина имеет для нас величайшее значение, мы не можем обойтись без строгого ее доказательства, хотя оно довольно сложно. Мы начнем со следующей леммы.

**Лемма.** *Если имеется два ряда чисел*

$$(I) \quad A, B, C, \dots$$

$$(II) \quad A', B', C', \dots$$

(одинаково ли количество членов в обоих рядах или нет — несущественно) с тем свойством, что если  $p$  обозначает простое число или степень простого числа и входит делителем хотя бы в один из членов второго ряда, то в первом ряду делятся на  $p$  по крайней мере столько же членов, сколько и во втором, то я утверждаю, что произведение всех чисел (I) делится на произведение всех чисел (II).

**Пример.** Если (I) состоит из чисел 12, 18, 45, а (II) — из чисел 3, 4, 5, 6, 9, то на числа 2, 4, 3, 9, 5 в (I) делятся соответственно 2, 1, 3, 2, 1 членов, а в (II) — соответственно 2, 1, 3, 1, 1 членов. Произведение же всех членов из (I), равное 9720, делится на произведение всех членов из (II), именно, на 3240.

**Доказательство.** Если произведение всех членов (I) равно  $Q$ , а произведение всех членов (II) равно  $Q'$ , то очевидно, что каждое

---

\* П. 98. Именно, очевидно, что  $a^2$  является вычетом по модулю  $q$ , не делимым на  $q$ , так как в противном случае на  $a$  делилось бы и простое число  $p$ , что невозможно.



простое число, которое является делителем  $Q'$ , будет также делителем  $Q$ . Покажем теперь, что каждый простой сомножитель числа  $Q'$  входит в  $Q$  по меньшей мере в той же степени, что и в  $Q'$ . Если  $p$  — такой делитель, и в ряде (I)  $a$  членов делятся на  $p$ ,  $b$  членов — на  $p^2$ ,  $c$  членов — на  $p^3$  и т. д., а буквы  $a'$ ,  $b'$ ,  $c'$ , ... имеют аналогичное значение для ряда (II), то легко видеть, что  $p$  имеет в  $Q$  степень  $a + b + c + \dots$ , а в  $Q'$  — степень  $a' + b' + c' + \dots$ . Но по предположению  $Q'$  не больше, чем  $a$ ,  $b'$  не больше, чем  $b$ , и т. д., и потому, очевидно,  $a' + b' + c' + \dots$  не больше чем  $a + b + c + \dots$ . Так как, таким образом, ни одно простое число не может входить в  $Q'$  в степени, большей, чем в  $Q$ , то  $Q$  делится на  $Q'$  (п. 17)

## 127

**Лемма.** В прогрессии  $1, 2, 3, 4, \dots, n$  на какое-нибудь число  $h$  может делиться не больше членов, чем в состоящем из стольких же членов ряде  $a, a + 1, a + 2, \dots, a + n - 1$ .

Именно, без труда видно, что если  $n$  есть кратность числа  $h$ , то в каждой из прогрессий на  $h$  делятся  $n/h$  членов. Если же это не так, то пусть  $n = eh + f$ , где  $f < h$ ; тогда в первом ряде на  $h$  будут делиться  $e$  членов, а во втором или столько же, или  $e + 1$  членов.

В качестве дополнения отсюда следует теорема, известная из теории фигурных чисел, но, если мы не ошибаемся, прямо еще никем не доказанная, именно, что

$$\frac{a(a+1)(a+2)\dots(a+n-1)}{1 \cdot 2 \cdot 3 \dots n}$$

всегда есть целое число.

Наконец, в более общем виде эту лемму можно было бы высказать так.

В прогрессии  $a, a + 1, a + 2, \dots, a + n - 1$  существует по меньшей мере столько же чисел, сравнимых с заданным числом  $r$  по модулю  $h$ , сколько среди чисел  $1, 2, 3, \dots, n$  имеется делящихся на  $h$ .

**Теорема.** Если  $a$  — какое-нибудь число вида  $8n + 1$ ,  $p$  — какое-нибудь взаимно простое с  $a$  число, по которому  $\pm a$  является вычетом, и, наконец,  $m$  — произвольное число, то я утверждаю, что в прогрессии

$$a, \frac{1}{2}(a - 1), 2(a - 4), \frac{1}{2}(a - 9), \dots, 2(a - m^2) \text{ или } \frac{1}{2}(a - m^2),$$

в зависимости от того, четно  $m$  или нечетно, существует по меньшей мере столько же членов, делящихся на  $p$ , сколько и в прогрессии.

$$1, 2, 3, \dots, 2m + 1.$$

Первую прогрессию мы обозначим через (I), вторую — через (II).

**Доказательство.** I. Если  $p = 2$ , то в (I) на  $p$  будут делиться все члены, за исключением первого, т. е.  $m$  членов; столько же членов будет делиться на  $p$  и в (II).

II. Если  $p$  — нечетное число, или удвоенное, или учетверенное нечетное число, и  $a \equiv r^2 \pmod{p}$ , то в прогрессии  $-m, -(m - 1), -(m - 2), \dots, +m$  (в которой столько же членов, сколько в (II), и которую мы обозначим через (III)) будет содержаться по меньшей мере столько же членов, сравнимых с  $r$  по модулю  $p$ , сколько в ряде (II) имеется членов, делящихся на  $p$  (согласно предыдущему пункту). Среди первых, однако, не может найтись никаких двух, которые отличались бы только знаком, но не абсолютной величиной\*. В то же время для каждого из них имеется соответствующий член в ряде (I), который делится на  $p$ . Именно, если  $\pm b$  — какой-нибудь член ряда (III), сравнимый с  $r$  по модулю  $p$ , то  $a - b^2$  будет делиться на  $p$ . Если теперь  $b$  четно, то член  $2(a - b^2)$  ряда (I) делится на  $p$ . Если же  $b$  нечетно, то на  $p$  делится член  $(a - b^2)/2$ ; действительно  $(a - b^2)/p$ , очевидно, будет четным целым числом, так как  $a - b^2$  делится на 8, а  $p$  — самое большее на 4 (в самом деле  $a$ , по предположению, имеет вид  $8n + 1$ , а  $r^2$ , будучи квадратом нечетного числа, имеет тот же самый вид, и следовательно, их раз-

---

\* Именно, если бы имело место  $r \equiv -f \equiv +f \pmod{p}$ , то на  $p$  делилось бы число  $2f$ , а значит (так как  $f^2 \equiv a \pmod{p}$ ), и число  $2a$ . Это возможно, однако, только тогда, когда  $p = 2$ , так как по предположению  $a$  взаимно просто с  $p$ . Случай же  $p = 2$  мы уже рассмотрели отдельно.

ность имеет вид  $8n$ ). Отсюда мы заключаем, наконец, что в ряде (I) делятся на  $p$  по крайней мере столько членов, сколько в ряде (III) имеется чисел, сравнимых с  $r$  по модулю  $p$ , т. е. столько же или больше, чем количество членов в (II), делящихся на  $p$ .

III. Пусть  $p$  имеет вид  $8n$  и  $a \equiv r^2 \pmod{2p}$ . (Действительно легко видеть, что так как  $a$ , по предположению, есть вычет числа  $p$ , оно будет вычетом и числа  $2p$ ). Тогда в ряде (III) будет по меньшей мере столько же членов, сравнимых с  $r$  по модулю  $p$ , сколько членов в (II) делится на  $p$ , и первые по абсолютной величине все будут различны. Но каждому из них в ряде (I) будет соответствовать член, делящийся на  $p$ . Действительно, если  $+b$  или  $-b \equiv r \pmod{p}$ , то  $b^2 \equiv r^2 \pmod{2p}$ \*, и потому член  $(a - b^2)/2$  делится на  $p$ . Тем самым в (I) существует по меньшей мере столько же членов, делящихся на  $p$ , сколько в (II).

## 129

**Теорема.** Если  $a$  — простое число вида  $8n + 1$ , то среди чисел, меньших  $2\sqrt{a} + 1$ , обязательно существует простое, по которому  $a$  является невычетом.

**Доказательство.** Пусть, если это возможно,  $a$  есть вычет всех простых чисел, которые меньше  $2\sqrt{a} + 1$ . Тогда легко видеть, что  $a$  будет также вычетом и всех составных чисел, которые меньше  $2\sqrt{a} + 1$  (в силу правил, по которым можно узнать, является ли данное число вычетом или невычетом составного числа; п. 105). Если наибольшее целое число, из тех, которые  $< \sqrt{a}$ , равно  $m$ , то в ряде

$$(I) \quad a, \frac{1}{2}(a - 1), 2(a - 4), \frac{1}{2}(a - 9), \dots, 2(a - m^2) \text{ или } \frac{1}{2}(a - m^2)$$

на любое число, меньшее  $2\sqrt{a} + 1$ , будет делиться по крайней мере столько же членов, сколько и в ряде

$$(II) \quad 1, 2, 3, 4, \dots, 2m + 1$$

(согласно предыдущему пункту).

---

\* Именно, число  $b^2 - r^2 = (b + r)(b - r)$  состоит из двух сомножителей, один из которых (по предположению) делится на  $p$ , а второй делится на 2 (так как и  $b$  и  $r$  нечетны); тем самым  $b^2 - r^2$  делится на  $2p$ .

Но отсюда следует, что произведение всех членов ряда (I) делится на произведение всех членов ряда (II) (п. 126). Первое же равно или  $a(a-1)(a-4)\dots(a-m^2)$ , или половине этого произведения (в зависимости от того, четно  $m$  или нечетно). Поэтому произведение  $a(a-1)(a-4)\dots(a-m^2)$  очевидно делится на произведение всех членов (II), а так как все эти члены взаимно просты с  $a$ , то на их произведение будет делиться и первое произведение, если отбросить от него сомножитель  $a$ . Но произведение всех членов (II) может быть представлено следующим образом:

$$(m+1)[(m+1)^2-1][(m+1)^2-4]\dots[(m+1)^2-m^2].$$

Поэтому

$$\frac{1}{m+1} \cdot \frac{a-1}{(m+1)^2-1} \cdot \frac{a-4}{(m+1)^2-4} \cdot \dots \cdot \frac{a-m^2}{(m+1)^2-m^2}$$

будет целым числом, хотя это есть произведение дробей, которые меньше 1; действительно, так как  $\sqrt{a}$  обязательно должно быть иррациональным, то  $m+1 > \sqrt{a}$  и потому  $(m+1)^2 > a$ . Отсюда следует, наконец, что наше предположение неверно.

Но так как  $a$ , очевидно,  $> 9$ , то  $2\sqrt{a} + 1 < a$ , и потому среди простых чисел, меньших  $a$ , существует такое, по которому  $a$  является невычетом.

**Индуктивным путем находится общая (фундаментальная) теорема и делаются выводы из нее**

После того как мы строго доказали, что каждое простое число вида  $4n+1$ , взятое как положительным, так и отрицательным, является невычетом некоторого простого числа, которое меньше его самого, мы тотчас же переходим к более подробному и общему сравнению простых чисел с точки зрения того, является ли одно из них вычетом или невычетом другого.

Выше мы со всей строгостью доказали, что  $-3$  и  $+5$  являются

вычетами или невычетами всех простых чисел, которые суть соответственно вычеты или невычеты чисел 3 или 5.

Из рассмотрения нижеследующих чисел мы находим, что  $-7$ ,  $-11$ ,  $+13$ ,  $+17$ ,  $-19$ ,  $-23$ ,  $+29$ ,  $-31$ ,  $+37$ ,  $+41$ ,  $-43$ ,  $-47$ ,  $+53$ ,  $-59$  и т. д. являются вычетами или невычетами всех простых чисел, которые, взятые положительными, являются для указанных чисел соответственно вычетами или невычетами. Это рассмотрение легко можно продолжить при помощи таблицы 2.

При некотором внимании каждый заметит, что из этих простых чисел те, которые имеют вид  $4n + 1$ , взяты с положительным знаком, а имеющие вид  $4n + 3$  — с отрицательным.

### 131

Мы скоро докажем, что найденное нами здесь индуктивным путем верно вообще. Однако прежде чем браться за это дело, нужно указать все, что следует из этой теоремы, если предположить ее справедливой. Саму теорему мы выскажем следующим образом.

*Если  $p$  — простое число вида  $4n + 1$ , то  $+p$ , а если  $p$  — простое число вида  $4n + 3$ , то  $-p$  будет вычетом или невычетом каждого простого числа, которое, взятое положительным, является вычетом или невычетом числа  $p$ .*

Так как почти все, что можно высказать о квадратичных вычетах, основывается на этой теореме, то название «фундаментальная теорема», которое мы в дальнейшем будем употреблять, не будет для нее неподходящим.

Чтобы наши выводы представить в возможно более краткой форме, мы будем обозначать через  $a$ ,  $a'$ ,  $a''$ , ... простые числа вида  $4n + 1$ , через  $b$ ,  $b'$ ,  $b''$ , ... — простые числа вида  $4n + 3$ , далее, через  $A$ ,  $A'$ ,  $A''$ , ... — любые числа вида  $4n + 1$  и через  $B$ ,  $B'$ ,  $B''$ , ... — любые числа вида  $4n + 3$ . Наконец, поставленная между двумя величинами буква  $R$  будет указывать, что первая является вычетом второй, а буква  $N$  будет иметь противоположное значение. Например,  $+5R11$ ,  $\pm 2N5$  означает соответственно, что  $+5$  есть вычет числа 11, а  $+2$  и  $-2$  суть невычеты числа 5. Если соединить теперь фундаментальную теорему с теоремами из п. 111, то легко получаются следующие теоремы.

| Если                                                               | То                                                              |
|--------------------------------------------------------------------|-----------------------------------------------------------------|
| 1) $\pm aRa'$                                                      | $\pm a'Ra$                                                      |
| 2) $\pm aNa'$                                                      | $\pm a'Na$                                                      |
| 3) $\left. \begin{array}{l} + aRb \\ - aNb \end{array} \right\}$   | $\pm bRa$                                                       |
| 4) $\left. \begin{array}{l} + aNb \\ - aRb \end{array} \right\}$   | $\pm bNa$                                                       |
| 5) $\pm bRa$                                                       | $\left\{ \begin{array}{l} + aRb \\ - aNb \end{array} \right.$   |
| 6) $\pm bNa$                                                       | $\left\{ \begin{array}{l} + aNb \\ - aRb \end{array} \right.$   |
| 7) $\left. \begin{array}{l} + bRb' \\ - bNb' \end{array} \right\}$ | $\left\{ \begin{array}{l} + b'Nb \\ - b'Rb \end{array} \right.$ |
| 8) $\left. \begin{array}{l} + bNb' \\ - bRb' \end{array} \right\}$ | $\left\{ \begin{array}{l} + b'Rb \\ - b'Nb \end{array} \right.$ |

132

Выше содержатся все случаи, которые могут встретиться при сравнении двух простых чисел; следующее касается любых чисел, однако доказательства здесь не так очевидны.

| Если          | То                                                            |
|---------------|---------------------------------------------------------------|
| 9) $\pm aRA$  | $\pm ARa$                                                     |
| 10) $\pm bRA$ | $\left\{ \begin{array}{l} + ARb \\ - ANb \end{array} \right.$ |
| 11) $+ aRB$   | $\pm BRa$                                                     |
| 12) $- aRB$   | $\pm BNa$                                                     |
| 13) $+ bRB$   | $\left\{ \begin{array}{l} - BRb \\ + BNb \end{array} \right.$ |
| 14) $- bRB$   | $\left\{ \begin{array}{l} + BRb \\ - BNb \end{array} \right.$ |

Так как доказательства всех этих теорем основываются на одних и тех же принципах, нет нужды все их подробно проводить; доказательство теоремы 9, которое мы приведем, может служить примером. Вообще же можно заметить, что каждое число вида  $4n + 1$  или совсем не имеет сомножителей вида  $4n + 3$ , или содержит два таких сомножителя, или четыре и т. д., т. е. что количество таких сомножителей (среди которых могут быть и равные) всегда четно, а каждое число вида  $4n + 3$ , напротив, всегда содержит нечетное число (т. е. или один или три, или пять и т. д.) сомножителей вида  $4n + 3$ . Число сомножителей вида  $4n + 1$  остается неопределенным.

Теорема 9 доказывается следующим образом. Пусть  $A$  есть произведение простых сомножителей  $a', a'', a''', \dots, b, b', b'', \dots$ , где число сомножителей  $b, b', b'', \dots$  четно (их может и не быть совсем, что сводится к тому же самому). Если теперь  $a$  является вычетом числа  $A$ , то оно будет также вычетом всех сомножителей  $a', a'', a''', \dots, b, b', b'', \dots$ , а потому, согласно теоремам 1 и 3 предыдущего пункта, эти отдельные сомножители, а, следовательно, и их произведение  $A$  являются вычетами числа  $a$ . Также и  $-A$  будет вычетом. Если же  $-a$  есть вычет числа  $A$ , а потому и отдельных сомножителей  $a', a'', \dots, b, b', \dots$ , то отдельные сомножители  $a', a'', \dots$  будут вычетами числа  $a$ , а сомножители  $b, b', \dots$  — невычетами. Так как, однако, количество последних четно, произведение всех сомножителей, т. е.  $A$ , будет вычетом числа  $a$ , а потому вычетом будет и  $-A$ .

### 133

*Мы еще обобщим наше исследование.* Рассмотрим два любых взаимно простых между собой нечетных числа  $P$  и  $Q$ , взятых с какими-нибудь знаками. Не обращая внимания на знак числа  $P$ , мы разложим его на простые сомножители, и обозначим через  $p$  количество тех из этих сомножителей, по которым  $Q$  является невычетом. Если некоторое простое число, по которому  $Q$  есть невычет, встречается среди этих  $p$  сомножителей несколько раз, то и учитывать его следует столько же раз. Аналогично, пусть  $q$  есть количество простых сомножителей числа  $Q$ , по которым  $P$  является невычетом. Тогда числа  $p$  и  $q$  находятся в некоторой связи одно с другим, которая зависит от природы чисел  $P, Q$ . Именно, если одно

из чисел  $p, q$  четно или нечетно, то по виду чисел  $P, Q$ , можно судить, будет ли второе четным или нечетным. Эта связь представлена в следующей таблице.

Числа  $p, q$  одновременно будут четными или нечетными, если числа  $P, Q$  имеют вид:

- 1)  $+A, +A'$ ;
- 2)  $+A, -A'$ ;
- 3)  $+A, +B$ ;
- 4)  $+A, -B$ ;
- 5)  $-A, -A'$ ;
- 6)  $+B, -B'$ .

Наоборот, одно из чисел  $p, q$  четно, а другое нечетно, когда числа  $P, Q$  имеет вид:

- 7)  $-A, +B$ ;
- 8)  $-A, -B$ ;
- 9)  $+B, +B'$ ;
- 10)  $-B, -B'$ .

**Пример.** Пусть числа  $P$  и  $Q$  суть  $-55$  и  $+1197$ , что относится к четвертому случаю. Здесь  $1197$  является невычетом одного единственного простого сомножителя числа  $55$ , именно, числа  $5$ , а  $-55$  есть невычет трех простых сомножителей числа  $1197$ , именно, чисел  $3, 3, 19$ .

Если  $P$  и  $Q$  обозначают простые числа, то эти теоремы переходят в те, которые мы привели в п. 131. Именно, в этом случае  $p$  и  $q$  могут быть не больше 1; если поэтому предположить, что  $p$  четно, оно обязательно будет  $= 0$ , т. е.  $Q$  будет вычетом числа  $P$ ; если же  $p$  нечетно, то  $Q$  есть невычет числа  $P$ , и обратно. Таким образом, если здесь вместо  $A, B$  написать  $a, b$ , то из 8) следует, что если  $-a$  есть вычет или невычет числа  $b$ ,  $-b$  будет невычетом или вычетом числа  $a$ , что совпадает с 3) и 4) из п. 131.

Вообще ясно, что  $Q$  может быть вычетом числа  $P$  только тогда, когда  $p = 0$ ; поэтому, если  $p$  нечетно, то  $Q$  заведомо есть невычет по модулю  $P$ .



Отсюда также могут быть без труда выведены теоремы предыдущего пункта.

Кстати, скоро станет ясно, что это общее рассмотрение является не просто бесплодным умозрением, так как полное доказательство фундаментальной теоремы едва ли может быть без него проведено.

### 134

*Мы приступаем теперь к выводу этих теорем.*

I. Мы будем, как и перед этим, считать, что  $P$ , на знак которого мы не обращаем внимания, разложено на простые сомножители, и разложим далее каким-нибудь образом также и  $Q$ , но уже учитывая его знак. Затем будем комбинировать каждый отдельный сомножитель первого разложения с каждым отдельным сомножителем второго разложения. Тогда, если  $s$  обозначает количество всех комбинаций, в которых сомножитель числа  $Q$  является невычетом сомножителя числа  $P$ , то  $p$  и  $s$  будут или одновременно четными, или одновременно нечетными. Действительно, если  $f, f', f'', \dots$  суть простые сомножители числа  $P$ , и если среди сомножителей, на которые разложено  $Q$ , имеется  $m$  невычетов по модулю  $f$ ,  $m'$  невычетов по модулю  $f'$ ,  $m''$  невычетов по модулю  $f''$  и т. д., то легко видеть, что

$$s = m + m' + m'' + \dots,$$

а  $p$  выражает, сколько среди чисел  $m, m', m'', \dots$  имеется нечетных. Отсюда сразу вытекает, что  $s$  будет четным, когда  $p$  четно, и нечетным, когда  $p$  нечетно.

II. Сказанное справедливо всегда, каким бы образом  $Q$  ни было разложено на сомножители. Теперь мы переходим к специальным случаям, и сначала рассмотрим случаи, когда одно из чисел,  $P$ , положительно, а другое,  $Q$ , имеет или вид  $+A$ , или вид  $-B$ . Разложим  $P$  и  $Q$  на простые сомножители, снабдив отдельные сомножители числа  $P$  положительными знаками, а отдельные сомножители числа  $Q$  — положительными или отрицательными знаками в зависимости от того, имеют ли они вид  $a$  или  $b$ ; тогда  $Q$ , очевидно, будет, как и требовалось, иметь или вид  $+A$ , или вид  $-B$ . Скомбинируем

отдельные сомножители числа  $P$  с отдельными сомножителями числа  $Q$  и обозначим, как и раньше, через  $s$  число комбинаций, в которых сомножитель  $Q$  является невычетом сомножителя  $P$ , и аналогично через  $t$  — число комбинаций, в которых сомножитель  $P$  является невычетом сомножителя  $Q$ . Тогда из фундаментальной теоремы следует, что первые комбинации совпадают со вторыми и потому  $s=t$ . Наконец, из только что доказанного следует, что  $p \equiv s \pmod{2}$ ,  $q \equiv t \pmod{2}$ , и потому  $p \equiv q \pmod{2}$ .

Тем самым мы получаем теоремы 1), 3), 4) и 6) из п. 133.

Остальные теоремы могут быть прямо выведены подобным же методом, но требуют одного нового соображения. Однако их легче получить из предыдущего следующим образом.

III. Обозначим снова через  $P$  и  $Q$  какие-нибудь взаимно простые нечетные числа, через  $p$  и  $q$  — количества простых сомножителей чисел  $P$ ,  $Q$ , по которым соответственно  $Q$  или  $P$  являются невычетами. Наконец, пусть  $p'$  — количество простых сомножителей числа  $P$ , по которым является невычетом —  $Q$  (если само  $Q$  отрицательно, то —  $Q$ , очевидно, будет обозначать положительное число). Разобьем теперь все простые сомножители числа  $P$  на четыре класса, именно

1) на сомножители вида  $a$ , по которым  $Q$  является вычетом;

2) на сомножители вида  $b$ , по которым  $Q$  является вычетом;

число их пусть равно  $\chi$ ;

3) на сомножители вида  $a$ , по которым  $Q$  является невычетом;

их число пусть равно  $\psi$ ;

4) на сомножители вида  $b$ , по которым  $Q$  является невычетом;

их число обозначим через  $\omega$ .

Тогда легко видеть, что  $p = \psi + \omega$ ,  $p' = \chi + \psi$ .

Если теперь  $P$  имеет вид  $\pm A$ , то  $\chi + \omega$ , а потому также и  $\chi - \omega$  будет четным числом; тем самым  $p' = p + \chi - \omega \equiv p \pmod{2}$ . Если же  $P$  имеет вид  $\pm B$ , то подобным же образом мы находим, что числа  $p$  и  $p'$  по модулю 2 несравнимы.

IV. Применим сказанное к отдельным случаям. Если сначала как  $P$ , так и  $Q$  имеют вид  $+A$ , то по теореме 1)  $p \equiv q \pmod{2}$ . Но, с другой стороны,  $p' \equiv p \pmod{2}$ , и потому  $p' \equiv q \pmod{2}$ , что совпадает с теоремой 2). Аналогично, если  $P$  имеет вид  $-A$ , а  $Q$  — вид  $+A$ , то, согласно только что доказанной теореме 2),

$p \equiv q \pmod{2}$ . Так как  $p' \equiv p$ , отсюда следует также  $p' \equiv q$ . Тем самым доказана также и теорема 5).

Тем же способом теорема 7) выводится из 3), теорема 8) — или из 4), или из 7), теорема 9) — из 6), и из нее же и теорема 10).

### Строгое доказательство фундаментальной теоремы

#### 135

Хотя в предыдущем пункте теоремы из п. 133 и не были доказаны, но было показано, что их справедливость следует из справедливости фундаментальной теоремы, которую мы пока лишь предположили. Но из самого способа вывода ясно, что эти теоремы верны для чисел  $P, Q$ , если только фундаментальная теорема имеет место для всех комбинаций простых сомножителей этих чисел, даже в том случае, если бы вообще она была и не верна.

*Мы будем говорить, что фундаментальная теорема верна до некоторого числа  $M$ , если она верна для любых двух простых чисел, ни одно из которых не превосходит  $M$ .*

Аналогичным образом нужно понимать выражения такого рода, что теоремы пп. 131, 132, 133 верны до некоторой границы. Легко видеть, что если доказана справедливость фундаментальной теоремы до некоторой границы, то и указанные теоремы в пределах этой границы имеют силу.

#### 136

Непосредственной проверкой легко можно показать, что для маленьких чисел фундаментальная теорема верна; таким путем определяется граница, до которой эта теорема заведомо верна. Мы предположим, что эта проверка произведена, причем совершенно безразлично, до какого места она сделана. Достаточно, например, установить справедливость теоремы только до числа 5; а это сразу видно, так как  $+5N3, \pm 3N5$ .

Если бы теперь фундаментальная теорема оказалась вообще, говоря, неверной, то существовала бы такая граница  $T$ , что до нее теорема вер-

на, а для следующего числа  $T+1$  она уже не верна. То же самое можно сказать по-иному, а именно, что существуют два простых числа, большее из которых есть  $T+1$ , которые находятся в противоречии с утверждением теоремы, но что для любых двух простых чисел, если оба они меньше  $T+1$ , теорема верна; отсюда следует, что до границы  $T$  верны и теоремы из пп. 131, 132, 133. Однако сейчас мы покажем, что это предположение не может быть верным. В соответствии с различными возможностями для вида числа  $T+1$  и того простого числа, которое меньше  $T+1$  и взятое с  $T+1$  противоречит утверждению теоремы, мы будем различать следующие случаи (при этом указанное простое число обозначим через  $p$ ).

Если и  $T+1$  и  $p$  имеют вид  $4n+1$ , то фундаментальная теорема могла бы быть не верна, если бы имело место одно из двух:

или одновременно  $\pm pR(T+1)$  и  $\pm (T+1)Nr$ ,

или одновременно  $\pm pN(T+1)$  и  $\pm (T+1)Rp$ .

Если и  $T+1$ , и  $p$  имеют вид  $4n+3$ , то фундаментальная теорема была бы не верна, если бы имело место

или одновременно  $+pR(T+1)$  и  $-(T+1)Nr$

(или, что сводится к тому же,  $-pN(T+1)$  и  $+(T+1)Rp$ ),

или одновременно  $+pN(T+1)$  и  $-(T+1)Rp$

(или  $-pR(T+1)$  и  $+(T+1)Nr$ ).

Если  $T+1$  имеет вид  $4n+1$ , а  $p$  — вид  $4n+3$ , то фундаментальная теорема не верна, если

или одновременно  $\pm pR(T+1)$  и  $+(T+1)Nr$  (или  $-(T+1)Rp$ ),

или одновременно  $\pm pN(T+1)$  и  $-(T+1)Nr$  (или  $+(T+1)Rp$ ).

Если  $T+1$  имеет вид  $4n+3$ , а  $p$  — вид  $4n+1$ , то фундаментальная теорема не верна, если

или одновременно  $+pR(T+1)$  (или  $-pN(T+1)$ ) и  $\pm (T+1)Nr$ ,

или одновременно  $+pN(T+1)$  (или  $-pR(T+1)$ ) и  $\pm (T+1)Rp$ .

Если может быть доказано, что ни один из этих восьми случаев не может иметь места, то мы тем самым, очевидно, получим, что справедливость фундаментальной теоремы не ограничена никакими пределами. К этому доказательству мы сейчас и приступаем. Но так как одни из этих случаев зависят от других, мы не будем придерживаться той же их последовательности, в которой они здесь перечислены.

## 137

**Первый случай.** Если  $T + 1$  имеет вид  $4n + 1 (= a)$ , и  $p$  — такого же вида, и, кроме того,  $\pm pRa$ , то не может быть  $\pm aNr$ . Выше этот случай фигурировал первым.

Пусть  $+p \equiv e^2 \pmod{a}$ , где  $e$  четно и меньше, чем  $a$  (чего всегда можно добиться). Тогда нужно различать два случая.

I. Если  $e$  не делится на  $p$ , то положим  $e^2 = p + af$ ; тогда  $f$  будет положительным числом вида  $4n + 3$  (т. е. вида  $B$ ), которое меньше  $a$  и не делится на  $p$ . Далее,  $e^2 \equiv p \pmod{f}$ , т. е.  $pRf$ , и потому, по теореме 11 из п. 132 (которую мы имеем право применить, так как  $p$  и  $f$  меньше, чем  $a$ , и значит, для них эти теоремы верны),  $\pm fRp$ . Но и  $afRp$ , откуда  $\pm aRp$ .

II. Если  $e$  делится на  $p$ , то положим  $e = gp$  и  $e^2 = p + arh$ , или  $pg^2 = 1 + ah$ . Тогда  $h$  имеет вид  $4n + 3$  ( $B$ ) и взаимно просто с  $p$  и  $g^2$ . Далее,  $pg^2Rh$  и потому также  $pRh$ , откуда (по теореме 11 из п. 132)  $\pm hRp$ . Но и  $-ahrp$ , ибо  $-ah \equiv 1 \pmod{p}$ . Следовательно,  $\pm aRp$ .

## 138

**Второй случай.** Если  $T + 1$  имеет вид  $4n + 1 (= a)$ ,  $p$  — вид  $4n + 3$ , и  $\pm pR(T + 1)$ , то не может быть  $+(T + 1)Nr$  или  $-(T + 1)Rp$ . Выше этот случай фигурировал пятым.

Пусть, как и выше,  $e^2 = p + fa$ , где  $e$  четно и меньше, чем  $a$ .

I. Если  $e$  не делится на  $p$ , то и  $f$  не будет делиться на  $p$ . Кроме того,  $f$  будет положительным числом, имеющим вид  $4n + 1$  (или  $A$ ), и меньшим, чем  $a$ . Далее,  $+pRf$  и потому (теорема 10 из п. 132)  $+fRp$ . Но и  $+faRp$ ; следовательно,  $+aRp$  или  $-aNp$ .

II. Если  $e$  делится на  $p$ , то пусть  $e = pg$  и  $f = ph$ . Поэтому  $g^2p = 1 + ha$ . Кроме того,  $h$  положительно, имеет вид  $4n + 3$  ( $B$ ) и взаимно просто с  $p$  и  $g^2$ . Далее,  $+g^2pRh$ , и поэтому  $+pRh$ . Следовательно (теорема 13 из п. 132),  $-hRp$ . Но  $-harp$ , откуда  $aRp$  и  $-aNp$ .

## 139

**Третий случай.** Если  $T + 1$  имеет вид  $4n + 1 (= a)$ ,  $p$  — число такого же вида, и  $\pm pNa$ , то не может быть  $\pm aRp$ . (Выше это был второй случай.)

Возьмем какое-нибудь простое число, меньшее, чем  $a$ , по которому  $\pm a$  является невычетом; то, что такое существует, мы уже раньше доказали (пп. 125, 129). При этом, однако, нужно отдельно рассматривать два случая, в зависимости от того, имеет ли это простое число вид  $4n + 1$  или  $4n + 3$ ; действительно, не было доказано, что существуют такие простые числа обоих этих видов.

I. Пусть указанное простое число имеет вид  $4n + 1$  и равно  $a'$ . Тогда  $\pm a'Na$  (п. 131), и потому  $\pm a'pRa$ . Пусть, таким образом,  $e^2 \equiv a'p \pmod{a}$ , где  $e$  четно и меньше чем  $a$ . Тогда снова нужно различать четыре случая.

1. Если  $e$  не делится ни на  $p$ , ни на  $a'$ , то положим  $e^2 = a'p \pm af$ , причем знак выбирается так, чтобы  $f$  было положительным. Тогда  $f$  будет  $< a$ , взаимно просто с  $a'$  и  $p$  и, если взять верхний знак, будет иметь вид  $4n + 3$ , а если нижний — вид  $4n + 1$ . Для краткости число простых сомножителей числа  $y$ , по которым  $x$  является невычетом, мы обозначим через  $[x, y]$ . Тогда  $a'pRf$ , и потому  $[a'p, f] = 0$ . Следовательно,  $[f, a'p]$  будет четным числом (теоремы 1) и 3) из п. 133), т. е. будет или равно 0, или равно 2. Поэтому  $f$  будет или вычетом обоих чисел  $a'$ ,  $p$ , или невычетом каждого из этих чисел. Первое, однако, невозможно, так как  $\pm af$  есть вычет числа  $a'$ , и  $\pm aNa'$  (по предположению), откуда  $\pm fNa'$ . Значит,  $f$  должно быть невычетом каждого из чисел  $a'$ ,  $p$ . Но вследствие  $\pm afRp$  будет  $\pm aNp$ , что и требовалось доказать.

2. Если  $e$  делится на  $p$ , но не делится на  $a'$ , то пусть  $e = pg$  и  $g^2p = a' \pm ah$ , причем знак берется такой, чтобы  $h$  было положительным. Тогда  $h$  будет  $< a$ , взаимно просто с  $a'$ ,  $g$  и  $p$  и в случае верхнего знака будет иметь вид  $4n + 3$ , а в случае нижнего — вид  $4n + 1$ . Из равенства  $g^2p = a' \pm ah$ , после умножения его на  $p$  и  $a'$ , без труда выводятся следующие соотношения:

$$(\alpha) \quad pa'Rh; \quad (\beta) \quad \pm ahpRa'; \quad (\gamma) \quad aa'hRp.$$

Из  $(\alpha)$  следует  $[pa', h] = 0$ , и потому (теоремы 1) и 3) из п. 133)  $[h, pa']$  четно, т. е.  $h$  является или вычетом, или невычетом обоих чисел  $p$ ,  $a'$  одновременно. В первом случае из  $(\beta)$  следует  $\pm apNa'$ , и так как по предположению  $\pm aNa'$ , будет  $\pm pRa'$ . Отсюда по фундаментальной теореме, которая верна для чисел  $p$ ,  $a'$ , меньших

$T + 1$ , получается, что  $\pm a'Rp$ . Из этого и из того, что  $hNp$ , следует, согласно  $(\gamma)$ ,  $\pm aNp$ , что и требовалось доказать. Во втором случае из  $(\beta)$  следует  $\pm apRa'$  и потому  $\pm pNa'$ ,  $\pm a'Np$  и, наконец, отсюда и из того, что  $hRp$ , получается, согласно  $(\gamma)$ ,  $\pm aNp$ .

3. Если  $e$  делится на  $a'$ , но не делится на  $p$ , то доказательство протекает почти точно также, как и в предшествующем случае, и не вызывает никаких новых трудностей.

4. Если  $e$  делится и на  $a'$ , и на  $p$ , а потому и на произведение  $a'p$  (действительно, мы можем считать, что числа  $a'$  и  $p$  различны между собой, так как иначе то, что мы хотим доказать, а именно, что  $aNp$ , уже содержалось бы в предположении  $aNa'$ ), то пусть  $e = ga'p$  и  $g^2a'p = 1 \pm ah$ . Тогда  $h$  будет меньше  $a$ , взаимно просто с  $a'$  и  $p$  и для верхнего знака имеет вид  $4n + 3$ , а для нижнего — вид  $4n + 1$ . Но легко видеть, что из последнего равенства вытекают следующие соотношения:

$$(\alpha) a'pRh; \quad (\beta) \pm ahRa'; \quad (\gamma) \pm ahRp.$$

Из соотношения  $(\alpha)$ , которое совпадает с  $(\alpha)$  во втором случае, вытекает, как и там, что одновременно имеет место или  $hRp$  и  $hRa'$ , или  $hNp$  и  $hNa'$ . Однако в первом случае, вследствие соотношения  $(\beta)$ , в противоречии с предположением было бы  $aRa'$ ; следовательно,  $hNp$ , и потому, в силу  $(\gamma)$ , также  $aNp$ .

II. Если указанное простое число имеет вид  $4n + 3$ , то доказательство настолько похоже на предыдущее, что проводить его излишне. Для тех, кто хочет сделать это самостоятельно (что мы очень рекомендуем), заметим только, что после того как они придут к равенству  $e^2 = bp \pm af$  (где  $b$  обозначает указанное простое число), ради достижения большей ясности следует рассматривать оба знака отдельно.

**Четвертый случай.** Если  $T + 1$  имеет вид  $4n + 1 (= a)$ ,  $p$  — вид  $4n + 3$ , и  $\pm pNa$ , то не может быть  $aRp$  или  $-aNp$ . (Выше этот случай был шестым.)

Это доказательство мы также ради краткости опускаем, так как оно совершенно аналогично доказательству третьего случая.

## 141

**Пятый случай.** Если  $T + 1$  имеет вид  $4n + 3 (= b)$ ,  $p$  имеет такой же вид, и  $+pRb$  или  $-pNb$ , то не может быть  $+bRp$  или  $-bNp$ . (Выше — третий случай.)

Пусть  $p \equiv e^2 \pmod{b}$ , где  $e$  четно и меньше, чем  $b$ .

I. Если  $e$  не делится на  $p$ , положим  $e^2 = p + bf$ . Тогда  $f$  будет положительным числом, меньшим  $b$ , взаимно простым с  $p$  и имеющим вид  $4n + 3$ . Далее, будет иметь место  $pRf$ , и потому, согласно теореме 13 из п. 132,  $-fRp$ . Отсюда и из того, что  $+bfRp$ , следует  $-bRp$ , и потому  $+bNp$ .

II. Если  $e$  делится на  $p$ , то пусть  $e = pg$  и  $g^2p = 1 + bh$ . Тогда  $h$  будет иметь вид  $4n + 1$  и будет взаимно просто с  $p$ , далее,  $p \equiv g^2p^2 \pmod{h}$ , и потому  $pRh$ . Отсюда получается  $+hRp$  (теорема 10 из п. 132), а из этого и из  $-bhRp$  следует  $-bRp$  или  $+bNp$ .

## 142

**Шестой случай.** Если  $T + 1$  имеет вид  $4n + 3 (= b)$ ,  $p$  — вид  $4n + 1$  и  $pRb$ , то не может быть  $\pm bNp$ . (Выше — седьмой случай.)

Доказательство, которое совершенно аналогично предыдущему, мы опускаем.

## 143

**Седьмой случай.** Если  $T + 1$  имеет вид  $4n + 3 (= b)$ ,  $p$  имеет такой же вид, и  $+pNb$  или  $-pRb$ , то не может быть  $+bNp$  или  $-bRp$ . (Выше — четвертый случай.)

Пусть  $-p \equiv e^2 \pmod{b}$ , где  $e$  четно и меньше, чем  $b$ .

I. Если  $e$  не делится на  $p$ , то пусть  $-p = e^2 - bf$ . Тогда  $f$  будет положительным числом вида  $4n + 1$ , взаимно простым с  $p$  и меньшим, чем  $b$  (действительно, очевидно, что  $e$  не больше  $b - 1$ , и  $p < b - 1$ , поэтому  $bf = e^2 + p < b^2 - b$ , т. е.  $f < b - 1$ ). Далее,  $-pRf$ , и потому (теорема 10 из п. 132)  $+fRp$ , а из этого и из того, что  $+bfRp$ , следует  $+bRp$  или  $-bNp$ .

II. Если  $e$  делится на  $p$ , то пусть  $e = pg$  и  $g^2p = -1 + bh$ . Тогда  $h$  будет положительным числом вида  $4n + 3$ , взаимно простым



с  $p$  и меньшим, чем  $b$ . Далее,  $-pRh$ , и потому (теорема 14 из п. 132)  $+hRp$ . Из этого и из того, что  $bhRp$ , следует  $+bRp$  или  $-bNp$ .

## 144

**Восьмой случай.** Если  $T + 1$  имеет вид  $4n + 3 (=b)$ ,  $p$  — вид  $4n + 1$ , и  $+pNb$  или  $-pRb$ , то не может быть  $\pm bRp$ . (Выше — последний случай.)

Доказательство проводится так же, как в предыдущем случае.

### Аналогичный метод для доказательства теоремы из п. 114

## 145

В предшествующих доказательствах мы все время предполагали значение числа  $e$  четным (пп. 137—144); заметим, что мы могли бы использовать и нечетные значения, но при этом нам пришлось бы отдельно рассматривать еще большее количество случаев. Те, которые находят в этом удовольствие, потрудятся не даром, если они потратят свои усилия на исследование этих случаев. Кроме того, тогда должны были бы предполагаться известными теоремы, касающиеся вычетов  $+2$  и  $-2$ . А так как наше доказательство было проведено без использования этих теорем, мы получаем тем самым новый способ для их доказательства. Этого не следует недооценивать, так как методы, которые мы использовали выше для доказательства теоремы о том, что  $\pm 2$  являются вычетами каждого простого числа вида  $8n + 1$ , оказываются несколько менее прямыми. Мы будем предполагать, что остальные случаи (в которых речь идет о простых числах вида  $8n + 3$ ,  $8n + 5$ ,  $8n + 7$ ) уже доказаны применявшимися выше методами, а эта теорема найдена только индуктивным путем; следующими далее рассуждениями мы докажем, что это индуктивное заключение действительно справедливо.

Если бы  $\pm 2$  не было бы вычетом всех простых чисел вида  $8n + 1$ , то пусть наименьшее простое число такого вида, для которого  $+2$

или  $-2$  является невычетом, было бы равно  $a$ , так что для всех простых чисел, меньших  $a$ , теорема справедлива. Возьмем тогда какое-нибудь простое число, меньшее, чем  $a/2$ , по которому  $a$  есть невычет (то, что такое число существует, легко получается из п. 129). Если оно равно  $p$ , то, согласно фундаментальной теореме, будет  $pNa$ . Поэтому  $\pm 2pRa$ . Пусть  $e^2 \equiv 2p \pmod{a}$ , где  $e$  нечетно и меньше, чем  $a$ . Тогда надо рассмотреть отдельно два случая.

I. Если  $e$  не делится на  $p$ , то пусть  $e^2 = 2p + aq$ . Тогда  $q$  будет положительным числом вида  $8n + 7$  или  $8n + 3$  (в зависимости от того, имеет ли  $p$  вид  $4n + 1$  или  $4n + 3$ ), меньшим, чем  $a$ , и не делящимся на  $p$ . Теперь разобьем все простые сомножители числа  $q$  на четыре класса; пусть при этом будет  $e$  сомножителей вида  $8n + 1$ ,  $f$  сомножителей вида  $8n + 3$ ,  $g$  сомножителей вида  $8n + 5$  и  $h$  сомножителей вида  $8n + 7$ ; пусть произведение всех сомножителей первого класса равно  $E$ , произведения всех сомножителей второго, третьего и четвертого классов равны соответственно  $F$ ,  $G$ ,  $H$  \*. После того как это сделано, рассмотрим сначала случай, когда  $p$  имеет вид  $4n + 1$  и потому  $q$  — вид  $8n + 7$ . Тогда легко видеть, что  $2RE$ ,  $2RH$ , и потому  $pRE$ ,  $pRH$ , откуда, наконец,  $ERp$ ,  $HRp$ . Далее,  $2$ , а потому и  $p$ , будут невычетами каждого сомножителя вида  $8n + 3$  или  $8n + 5$ ; поэтому каждый такой сомножитель будет невычетом числа  $p$ , откуда легко следует, что  $FG$  будет вычетом числа  $p$ , если  $f + g$  четно, и невычетом, если  $f + g$  нечетно. Но  $f + g$  не может быть нечетным; действительно, разбором всевозможных случаев легко убедиться, что если  $f + g$  нечетно, то  $EFGH$ , или  $q$ , будет иметь или вид  $8n + 3$ , или вид  $8n + 5$ , каковы бы ни были  $e$ ,  $f$ ,  $g$ ,  $h$  в отдельности, что противоречит предположению. Следовательно,  $FGRp$ ,  $EFGHRp$ , или  $qRp$ , и отсюда, в силу  $aqRp$ , вытекает, наконец,  $aRp$ , что находится в противоречии с предположением. Если же  $p$  имеет вид  $4n + 3$ , то подобным же образом можно показать, что  $pRE$  и потому  $ERp$ , —  $pRF$ , откуда  $FRp$ ,  $q + h$  четно, и потому, наконец, вопреки предположению,  $qRp$ ,  $aRp$ .

---

\* Когда совсем нет сомножителей, принадлежащих некоторому классу, вместо их произведения нужно писать 1.

II. Если  $e$  делится на  $p$ , то доказательство может быть проведено подобным же образом, и для опытного читателя (а этот пункт написан специально для таких) не представит затруднений. Ради краткости мы его опускаем.

## Решение общей проблемы

146

При помощи фундаментальной теоремы и теорем, относящихся к вычетам  $-1$  и  $\pm 2$ , всегда можно определить, является ли какое-нибудь заданное число вычетом или невычетом заданного простого числа. Не будет бесполезным еще раз повторить здесь и другие факты, изложенные выше, чтобы иметь вместе все необходимое для решения следующего вопроса.

**Задача.** Пусть даны любые два числа  $P, Q$ ; определить, является ли  $Q$  вычетом или невычетом по модулю  $P$ .

**Решение.** I. Пусть  $P = a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные положительные (ибо  $P$  можно считать положительным) простые числа. Для краткости мы будем здесь называть просто отношением числа  $x$  к числу  $y$  ту связь между ними, которая проявляется в том, что  $x$  является вычетом или невычетом по модулю  $y$ . Отношение  $Q$  к  $P$  зависит, таким образом, от отношений  $Q$  к  $a^\alpha$ ,  $Q$  к  $b^\beta$  и т. д. (п. 105).

II. Чтобы уметь узнавать отношение  $Q$  к  $a^\alpha$  (для других пар,  $Q, b^\beta$  и т. д., дело обстоит так же), нужно разобрать два случая.

1. Если  $Q$  делится на  $a$ , то положим  $Q = Q'a^e$ , где  $Q'$  уже не делится на  $a$ . Если тогда  $e = \alpha$  или  $e > \alpha$ , то  $QRa^\alpha$ ; если  $e < \alpha$  и нечетно, то  $QNa^\alpha$ ; наконец, если  $e < \alpha$  и четно, то отношение  $Q$  к  $a^\alpha$  будет таким же, что и отношение  $Q'$  к  $a^{\alpha-e}$ . Следовательно, этот случай сводится к случаю, когда

2.  $Q$  не делится на  $a$ . Здесь мы снова будем различать два случая.

(A).  $a = 2$ . Тогда при  $\alpha = 1$  всегда  $QRa^\alpha$ ; если  $\alpha = 2$ , то нужно, чтобы  $Q$  имело вид  $4n + 1$ ; наконец, если  $\alpha = 3$  или  $\alpha > 3$ , то  $Q$  должно иметь вид  $8n + 1$ . Если это условие выполнено, то  $QRa^\alpha$ .

(B).  $a$  — какое-нибудь другое простое число. Тогда отношение  $Q$  к  $a^2$  такое же, как и  $Q$  к  $a$  (ср. п. 101).

III. Отношение любого числа  $Q$  к (нечетному) простому числу  $a$  определяется следующим образом. Если  $Q > a$ , то вместо  $Q$  подставляется его наименьший положительный вычет\* по модулю  $a$ . Отношение этого вычета к  $a$  такое же, как и числа  $Q$  к  $a$ .

Далее, число  $Q$ , или то, которым оно заменено, разлагается на простые сомножители  $p, p', p'', \dots$ , к которым добавляется еще множитель  $-1$ , если  $Q$  отрицательно. Тогда, как известно, отношение  $Q$  к  $a$  зависит от отношений отдельных сомножителей к  $a$ . Именно, если среди этих сомножителей имеется  $2m$  невычетов числа  $a$ , то  $QRa$ , а если невычетов  $2m + 1$ , то  $QNa$ . При этом легко видеть, что если среди сомножителей  $p, p', p'', \dots$  имеется два, или четыре, или шесть, или, вообще,  $2k$  совпадающих, то их можно просто отбрасывать.

IV. Если среди сомножителей  $p, p', p'', \dots$  встречаются  $-1$  и  $2$ , то отношение их к  $a$  определяется из пп. 108, 112, 113, 114. А отношения остальных сомножителей к  $a$  зависят от отношений  $a$  к этим сомножителям (фундаментальная теорема и теоремы из п. 131). Если  $p$  — один из них, то можно убедиться (рассматривая числа  $a$  и  $p$  так же, как перед этим числа  $Q$  и  $a$ , которые соответственно больше их), что отношение  $a$  к  $p$  или может быть определено в соответствии с пп. 108—114 (именно, если наименьший вычет числа  $a$  по модулю  $p$  не имеет нечетных простых сомножителей), или еще зависит от отношений  $p$  к некоторым простым числам, которые меньше  $p$ . То же самое имеет место и для остальных сомножителей  $p', p'', \dots$ . Легко видеть, что, продолжая этот процесс, мы в конце концов придем к числам, отношения между которыми можно определить при помощи теорем из пп. 108—114. На примере это будет яснее.

Пример. Отыскивается отношение числа  $+453$  к  $1236$ . Имеем:  $1236 = 4 \cdot 3 \cdot 103$ ;  $453 \ R 4$ , согласно II, 2 (A);  $+453 \ R 3$ , согласно II, 1. Остается, таким образом, получить только отношение  $+453$  к  $103$ . Оно будет таким же, что и отношение  $+41 (\equiv 453 \pmod{103})$  к  $103$ .

---

\* «Вычет» в смысле п. 4. — Часто бывает лучше брать абсолютно наименьший вычет.

Последнее в свою очередь такое же (по фундаментальной теореме), как отношение  $+103$  к  $41$  или  $-20$  к  $41$ . Но  $-20R41$ ; действительно,  $-20 = -1 \cdot 2 \cdot 2 \cdot 5$ ;  $-1R41$  (п. 108) и  $+5R41$ , ибо (фундаментальная теорема)  $41 \equiv 1$ , и потому является вычетом числа  $5$ . Отсюда следует  $+453R103$ , откуда, наконец,  $+453R1236$ . Действительно,  $453 \equiv 297^2 \pmod{1236}$ .

**О линейных формах, содержащих все простые числа,  
по которым заданное число является вычетом  
или невычетом**

147

Если дано любое число  $A$ , то можно указать определенные формулы, в которых содержатся все взаимно простые с  $A$  числа, по которым  $A$  является вычетом, т. е. все числа, которые могут быть делителями чисел вида  $x^2 - A$  (где  $x^2$  обозначает произвольный квадрат)\*. Для краткости мы рассмотрим только нечетные делители, взаимно простые с  $A$ , так как остальные случаи легко могут быть сведены к этому.

Пусть сначала  $A$  — или простое число вида  $4n + 1$ , взятое положительным, или простое число вида  $4n - 1$ , взятое со знаком  $-$ . Тогда, в силу фундаментальной теоремы, все те простые числа, которые, будучи взяты положительными, являются вычетами числа  $A$ , будут делителями  $x^2 - A$ , а все простые числа (за исключением числа  $2$ , которое всегда есть делитель), являющиеся невычетом для  $A$ , не будут делить  $x^2 - A$ . Обозначим все вычеты числа  $A$ , меньшие, чем  $A$  (за исключением нуля), через  $r, r', r'', \dots$ , а все невычеты — через  $n, n', n'', \dots$ . Тогда каждое простое число, содержащееся в одной из форм  $Ak + r, Ak + r', Ak + r'', \dots$ , будет делителем  $x^2 - A$ , а каждое простое число, содержащееся в одной из форм  $Ak + n, Ak + n', Ak + n'', \dots$ , не делит  $x^2 - A$ ; здесь  $k$  обозначает произвольное целое число. Первые формы мы будем называть формами делителей, а вторые — формами неделителей выражения  $x^2 - A$ .

---

\* Такие числа мы будем называть просто делителями выражения  $x^2 - A$ ; тем самым становится само собой понятным, что такое «неделители».

Число тех и других одинаково и равно  $(A - 1)/2$ . Если, далее,  $B$  — нечетное составное число, и  $ARB$ , то все простые сомножители числа  $B$ , а потому и само  $B$ , будут содержаться в одной из первых форм. Следовательно, каждое нечетное число, содержащееся в одной из форм делителей, не будет делить  $x^2 - A$ . Однако обратное утверждение неверно; действительно, если  $B$  есть нечетный составной делитель выражения  $x^2 - A$ , то среди простых сомножителей числа  $B$  будет несколько делителей, но если количество их четно, то само  $B$  будет находиться в какой-нибудь форме делителей (ср. п. 99).

**Пример.** Для  $A = -11$  указанным способом находим, что формы делителей выражения  $x^2 + 11$  суть  $11k + 1, 3, 4, 5, 9$ , а формы делителей:  $11k + 2, 6, 7, 8, 10$ . Поэтому  $-11$  будет невычетом всех нечетных чисел, содержащихся в одной из последних форм, и вычетом всех простых чисел, принадлежащих к какой-нибудь из первых форм.

Такие же формы существуют и для делителей и делителей выражения  $x^2 - A$ , где  $A$  — любое число. Легко видеть, однако, что нужно рассматривать только такие значения  $A$ , которые не делятся ни на какой квадрат; действительно, если  $A = a^2 A'$ , то все делители  $x^2 - A$  будут, очевидно, и делителями  $x^2 - A'$ , и то же самое имеет место для делителей. Мы будем различать три случая: 1) случай, когда  $A$  имеет вид  $+(4n + 1)$  или  $-(4n - 1)$ , 2) случай, когда  $A$  имеет вид  $-(4n + 1)$  или  $+(4n - 1)$ , 3) случай, когда  $A$  четно, т. е. имеет вид  $\pm (4n + 2)$ .

**Первый случай:**  $A$  имеет вид  $+(4n + 1)$  или  $-(4n - 1)$ . Разложим  $A$  на простые сомножители, и те из них, которые имеют вид  $4n + 1$ , снабдим положительным знаком, а имеющие вид  $4n - 1$  — отрицательным знаком (от чего произведение не изменится, т. е. по-прежнему будет равно  $A$ ). Пусть эти сомножители суть  $a, b, c, d, \dots$ . Разобьем далее все числа, которые меньше  $A$  и взаимно просты с  $A$ , на два класса, причем в первом классе соберем все числа, которые являются невычетами или ни для одного, или для двух, или для

---

\* Имеются в виду делители, взаимно простые с  $A$ .

четырех, вообще, для четного количества чисел среди  $a, b, c, d, \dots$ , а во втором — числа, являющиеся невычетами или для одного, или для трех, вообще, для нечетного количества чисел среди  $a, b, c, d, \dots$ . Первые обозначим через  $r, r', r'', \dots$ , а вторые — через  $n, n', n'', \dots$ . Тогда формы  $Ak + r, Ak + r', Ak + r'', \dots$  будут формами делителей выражения  $x^2 - A$ , а формы  $Ak + n, Ak + n', Ak + n'', \dots$  — формами неделителей  $x^2 - A$  (т. е. *каждое простое число, кроме 2, будет делителем или неделителем выражения  $x^2 - A$ , в зависимости от того, содержится ли оно в одной из первых, или в одной из вторых форм*). Действительно, если  $p$  — простое число, взятое положительным, которое по одному из чисел  $a, b, c, \dots$  является вычетом или невычетом, то и само это число будет соответственно вычетом или невычетом числа  $p$  (в силу фундаментальной теоремы). Поэтому, если среди  $a, b, c, \dots$  имеется  $t$  чисел, по которым  $p$  есть невычет, то среди них будет и  $t$  невычетов числа  $p$ , и потому, если  $p$  содержится в одной из первых форм,  $t$  будет четным, и  $ARp$ , а если в одной из вторых форм, то  $t$  нечетно, и  $ANp$ .

**Пример.** Пусть  $A = +105 = (-3) \cdot (+5) \cdot (-7)$ . Тогда числа  $r, r', r'', \dots$  будут следующие: 1, 4, 16, 46, 64, 79 (которые не являются невычетами ни одного из чисел 3, 5, 7); 2, 8, 23, 32, 53, 92 (которые являются невычетами чисел 3, 5); 26, 41, 59, 89, 101, 104 (которые являются невычетами чисел 3, 7); 13, 52, 73, 82, 97, 103 (которые являются невычетами чисел 5, 7). Числа же  $n, n', n'', \dots$  будут следующие: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Первые шесть являются невычетами числа 3, шесть следующих суть невычеты числа 5; затем следуют невычеты числа 7, и наконец, те, числа, которые одновременно являются невычетами всех трех.

Из комбинаторных соображений и из пп. 32 и 96 легко выводится, что количество чисел  $r, r', r'', \dots$  равно

$$t \left( l + \frac{l(l-1)}{1 \cdot 2} + \frac{l(l-1)(l-2)(l-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \dots \right),$$

а количество чисел  $n, n', n'', \dots$  равно

$$t \left( l + \frac{l(l-1)(l-2)}{1 \cdot 2 \cdot 3} + \frac{l(l-1)(l-2)(l-3)(l-4)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} + \dots \right),$$

где  $l$  обозначает количество чисел  $a, b, c, \dots$ ,

$$t = 2^{-l}(a-1)(b-1)(c-1)\dots,$$

и оба ряда продолжаются до тех пор, пока не оборвутся. (Действительно, имеется  $t$  чисел, являющихся невычетами всех чисел  $a, b, c, \dots$ ,  $t \cdot l \cdot (l-1) / 1 \cdot 2$  чисел, являющихся невычетами двух из них, и т. д.; однако необходимость краткости не позволяет нам проводить это доказательство подробнее.) Сумма же каждого из этих рядов \* равна  $2^{l-1}$ . Для первого ряда это можно получить, объединяя в выражении

$$1 + (l-1) + \frac{(l-1)(l-2)}{1 \cdot 2} + \dots$$

второй член с третьим, четвертый с пятым, и т. д., а для второго — объединяя в этом же выражении первый член со вторым, третий с четвертым и т. д. Таким образом, количества форм делителей и форм неделителей выражения  $x^2 - A$  одинаковы, именно равны  $\frac{1}{2}(a-1)(b-1)(c-1)\dots$ .

#### 149

**Второй и третий случаи мы можем рассмотреть одновременно.** Именно, здесь всегда можно положить  $A$  равным или  $(-1)Q$ , или  $(+2)Q$ , или  $(-2)Q$ , где  $Q$  есть число вида  $+(4n+1)$  или  $-(4n-1)$ , которое мы рассмотрели в предыдущем пункте. Пусть вообще  $A = \alpha Q$ , так что  $\alpha$  или равно  $-1$ , или равно  $\pm 2$ . Тогда  $A$  есть вычет всех чисел, по которым оба числа  $\alpha$  и  $Q$  одновременно являются вычетами или невычетами, и невычетом всех чисел, по которым только одно из чисел  $\alpha$  и  $Q$  является невычетом. Отсюда легко вывести формы делителей и неделителей выражения  $x^2 - A$ . Если  $\alpha = -1$ , то все числа, которые меньше, чем  $4A$  и взаимно просты с этим числом, мы разобьем на два класса, относя к первому классу те числа, которые содержатся в какой-нибудь форме делителей выражения  $x^2 - Q$  и одновременно имеют вид  $4n+1$ , а также те, которые содержатся в какой-нибудь форме неделителей выра-

---

\* После отбрасывания сомножителя  $t$ .



жения  $x^2 - Q$  и одновременно имеют вид  $4n + 3$ ; все остальные числа отнесем ко второму классу. Если числа первого класса суть  $r, r', r'', \dots$ , а числа второго класса —  $n, n', n'', \dots$ , то  $A$  будет вычетом всех простых чисел, содержащихся в одной из форм  $4Ak + r, 4Ak + r', 4Ak + r'', \dots$ , и невычетом всех простых чисел, содержащихся в формах  $4Ak + n, 4Ak + n', \dots$ . Если  $\alpha = \pm 2$ , то мы будем разбивать на два класса все числа, которые меньше, чем  $8Q$  и взаимно просты с  $4Q$ , причем к первому классу будем относить все числа, которые содержатся в одной из форм делителей выражения  $x^2 - Q$  и одновременно, в случае верхнего знака, имеют вид  $8n + 1$  или  $8n + 7$ , а в случае нижнего знака — вид  $8n + 3$  или  $8n + 5$ , и все числа, которые содержатся в одной из форм неделителей выражения  $x^2 - Q$  и одновременно, в случае верхнего знака, имеют вид  $8n + 3$  или  $8n + 5$ , а в случае нижнего знака — вид  $8n + 1$  или  $8n + 7$ ; все остальные числа отнесем ко второму классу. Если тогда числа первого класса обозначить через  $r, r', r'', \dots$ , а числа второго класса — через  $n, n', n'', \dots$ , то  $\pm 2Q$  будет вычетом всех простых чисел, содержащихся в одной из форм  $8Qk + r, 8Qk + r', 8Qk + r'', \dots$ , и невычетом всех простых чисел, содержащихся в одной из форм  $8Qk + n, 8Qk + n', 8Qk + n'', \dots$ . Легко также доказать, что и здесь имеется одинаковое количество форм делителей и форм неделителей выражения  $x^2 - A$ .

**Пример.** Этим способом можно найти, что  $+10$ , есть вычет всех простых чисел, содержащихся в одной из форм  $40k + 1, 3, 9, 13, 27, 31, 37, 39$ , и невычетом всех простых чисел, содержащихся в одной из форм  $40k + 7, 11, 17, 19, 21, 23, 29, 33$ .

Эти формы обладают многими замечательными свойствами, из которых мы здесь укажем одно. Если  $B$  есть составное взаимно простое с  $A$  число, среди простых сомножителей которого имеется  $2m$  таких, которые содержатся в формах неделителей выражения  $x^2 - A$ , то  $B$  содержится в одной из форм делителей этого выражения; если же число простых сомножителей числа  $B$ , которые содержатся в формах неделителей выражения  $x^2 - A$ , нечетно, то и  $B$  бу-

дет содержаться в одной из форм неделителей. Несложное доказательство мы опускаем. Из этого следует, что не только каждое простое число, но и каждое составное нечетное взаимно простое с  $A$  число, которое содержится в одной из форм неделителей, само является неделителем; действительно, один из простых сомножителей такого числа обязательно должен быть неделителем.

### О работах других авторов, относящихся к этим исследованиям

151

Фундаментальная теорема, которая, без сомнения, должна быть причислена к наиболее изящным открытиям в этой области, в той простой форме, в которой мы ее дали выше, ранее никем не была высказана. Этому следует удивляться тем более, что некоторые другие теоремы, которые из нее вытекают и из которых ее в свою очередь легко было бы вывести, были уже известны Эйлеру. Он знал, что существуют формы, в которых содержатся все простые делители чисел вида  $x^2 - A$ , и формы, в которых содержатся все их простые неделители, причем все первые формы отличны от всех вторых, и указал способ находить такие формы; однако все его попытки получить доказательство были тщетны и лишь приводили к тому, что истины, найденные индуктивным путем, становились более вероятными. Правда, в одном своем сочинении, «*Novae demonstrationes circa divisores numerorum formae  $x^2 + my^2$* » (которое поступило в Петербургскую Академию 20 ноября 1775 г. и было издано уже после смерти этого выдающегося математика в первом томе «*Nova Acta*» этой Академии), как видно из стр. 47 и следующих, он, по-видимому, считал, что доказательство ему удалось; но здесь вкралась ошибка, так как на стр. 65 он молчаливо предполагает, что формы делителей и неделителей существуют\*, из чего уже нетрудно было вывести, какой они

---

\* Именно, что существуют числа  $r, r', r'', \dots, n, n', n'', \dots$ , которые все различны, меньше, чем  $4A$ , и обладают тем свойством, что все простые делители выражения  $x^2 - A$  содержатся в одной из форм  $4Ak + r, 4Ak + r', \dots$ , а все простые неделители — в одной из форм  $4Ak + n, 4Ak + n', \dots$ , (где  $k$  — обозначает произвольное число).

должны иметь вид. Однако метод, который он использует для обоснования указанного предположения, едва ли пригоден. В другом сочинении: «*De criteriis aequationis  $fx^2 + gy^2 = hz^2$  untrumque resolutionem admittat necne*», *Opusc. Analyt. T. I.* (где  $f, g, h$  являются заданными, а  $x, y, z$  — неизвестными числами) он индуктивным путем находит, что если для  $h = s$  уравнение разрешимо, то оно разрешимо и для всякого значения, сравнимого с  $s$  по модулю  $4fg$ , если только оно является простым числом; на основании этой теоремы предположение, о котором идет речь, легко может быть доказано. Однако доказательство этой теоремы также не поддалось всем его усилиям \*, что и не удивительно, так как, по нашему мнению, следовало исходить из фундаментальной теоремы. Справедливость этой теоремы будет сама собой вытекать из того, что мы изложим в следующем разделе.

После Э й л е р а этим вопросом в своем замечательном труде «*Recherches d'analyse indéterminée*», *Hist. de l'Acad. des Sc., 1785, p. 465*, занимался Л е ж а н д р. Он получил (стр. 465) теорему, которая по сути дела идентична фундаментальной теореме; именно, если  $p$  и  $q$  — два положительных простых числа, то если одно из них имеет вид  $4n + 1$ , то абсолютные наименьшие вычеты степеней  $p^{(q-1)/2}$  и  $q^{(p-1)/2}$  соответственно по модулям  $q$  и  $p$  или оба равны  $+1$ , или оба равны  $-1$ ; если же  $p$  и  $q$  оба имеют вид  $4n + 3$ , то один из этих абсолютно наименьших вычетов равен  $+1$ , а другой равен  $-1$ ; согласно п. 106, отсюда следует, что отношения (в смысле п. 146)  $p$  к  $q$  и  $q$  к  $p$  одинаковы, когда хотя бы одно из чисел  $p$  и  $q$  имеет вид  $4n + 1$ , и противоположны, когда и  $p$ , и  $q$  имеют вид  $4n + 3$ . Эта теорема содержится среди теорем из п. 131; она следует также из теорем 1, 3, 9 п. 133; в свою очередь, фундаментальная теорема может

---

\* Как он свидетельствует и сам в цитированном сочинении, стр. 216: «*Hujus elegantissimi theorematis demonstratio adhuc desiteratur, postquam a pluribus jamcludum frustra est investigata... Quocirca plurimum is praestitisse censendus est, cui successerit demonstrationem hujus theorematis invenire*». С какой настойчивостью этот бессмертный математик стремился получить доказательства этой теоремы и других предложений, являющихся лишь частными случаями фундаментальной теоремы, видно из многих других мест «*Opusc. Analyt.*» (ср. «*Additamentum ad. diss.*», VIII, T. I и *diss. XIII, T. II*, а также многие сочинения в «*Comment. Ac. Petrop.*», которые мы уже упоминали).

быть выведена из нее. Л е ж а н д р попытался также дать доказательство, о котором, так как оно весьма остроумно, мы будем подробнее говорить в следующем разделе. Так как, однако, он принимал без доказательства многие утверждения (о чем он сам говорит на стр. 520: «*Nous avons supposé seulement...*»), часть из которых до сих пор вообще никем не была доказана, а часть, по крайней мере на наш взгляд, и не может быть доказана без помощи фундаментальной теоремы, то избранный им путь, по-видимому, не в состоянии привести к цели, и потому наше доказательство должно считать первым\*. Впрочем, в дальнейшем мы изложим еще два других доказательства этой в высшей степени важной теоремы, которые совершенно отличны и от приведенного выше доказательства и между собой.

## О сравнениях второй степени общего вида

### 152

До сих пор мы рассматривали «чистое» сравнение  $x^2 \equiv A \pmod{m}$  и показали, как можно решить вопрос о том, разрешимо ли оно. Отыскание самих корней было, в силу п. 105, сведено к случаю, когда  $m$  является или простым числом, или степенью простого числа, а вторая из этих возможностей, согласно п. 101, также сводится к тому случаю, когда  $m$  есть простое число. В отношении же этого последнего случая почти все, что может быть получено прямыми методами, охватывается изложенным в пп. 61 и следующих, в соединении с тем, что мы рассмотрим в пятом и шестом разделах. Вообще же, эти прямые методы, если и оказываются применимыми, все же в большинстве случаев бывают намного длиннее косвенных, которые мы изложим в разделе VI, и потому достойны внимания не столько с точки зрения практической пользы, сколько вследствие своей красоты.

*Произвольные сравнения второй степени легко могут быть сведены к чистым сравнениям.* Если дано сравнение

$$ax^2 + bx + c \equiv 0,$$

---

\* Ср. дополнения в конце «Исследований».

которое должно быть решено по модулю  $m$ , то ему эквивалентно сравнение

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am},$$

т. е. каждое число, удовлетворяющее одному из этих сравнений, удовлетворяет и другому. Второе же сравнение может быть представлено в виде

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am},$$

откуда все значения  $2ax + b$ , которые меньше, чем  $4am$ , могут быть найдены, если только они вообще существуют. Если эти значения обозначить через  $r, r', r'', \dots$ , то все решения заданного сравнения получаются из решений сравнений

$$2ax \equiv r - b, \quad 2ax \equiv r' - b, \quad \dots \pmod{4am},$$

которые мы научились находить во втором разделе. Впрочем, следует заметить, что в большинстве случаев решение может быть упрощено применением различных специальных приемов; например, вместо заданного сравнения бывает возможно подыскать равносильное ему сравнение

$$a'x^2 + 2b'x + c' \equiv 0,$$

в котором  $a'$  входит в  $m$ ; однако ради краткости мы не будем излагать здесь это подробно, тем более, что с этими вопросами мы еще встретимся в последнем разделе.

---

## Р А З Д Е Л V

### О ФОРМАХ И НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЯХ ВТОРОЙ СТЕПЕНИ

Предмет исследования; определение форм и обозначения

153

В этом разделе мы будем главным образом заниматься функциями двух переменных  $x, y$  следующего вида:

$$ax^2 + 2bxy + cy^2,$$

где  $a, b, c$  являются заданными целыми числами, и будем называть эти функции **формами второй степени или просто формами**. Это исследование достигает своей вершины в решении знаменитой проблемы об отыскании всех решений любого неопределенного уравнения второй степени с двумя неизвестными, когда эти неизвестные должны принимать либо целые, либо лишь рациональные значения. Правда, эта проблема решена еще **Л а г р а н ж е м**, и многое, касающееся природы форм, было как этим великим математиком, так и **Э й л е р о м**, частью впервые найдено, частью же доказано после того, как это было найдено **Ф е р м а**. Однако при основательном исследовании форм нам открылось так много нового, что нам показалось целесообразным заново изложить весь этот предмет, тем более, что открытое указанными математиками разбросано во многих местах, и, как нам кажется, было известно лишь немногим; затем, способ

изложения этого предмета в большинстве случаев является нашим собственным, и, наконец, открытое нами вряд ли было бы понятно без нового изложения, сделанного ранее. Однако, несомненно, что в этом вопросе еще остается неоткрытым много замечательного, к чему могут приложить свои силы другие. Впрочем, относящееся к истории отыскания наиболее выдающихся свойств мы всегда будем указывать в соответствующих местах.

Форму  $ax^2 + 2bxy + cy^2$ , когда дело не будет касаться самих неизвестных  $x, y$ , мы будем обозначать через  $(a, b, c)$ . Таким образом, это выражение будет обозначать произвольную сумму трех слагаемых, именно, произведения заданного числа  $a$  на квадрат любого неизвестного, удвоенного произведения числа  $b$  на это неизвестное и некоторое другое неизвестное и, наконец, произведения числа  $c$  на квадрат этого второго неизвестного. Например,  $(1, 0, 2)$  будет представлять сумму квадрата и удвоенного квадрата. Далее, хотя формы  $(a, b, c)$  и  $(c, b, a)$  обозначают одно и то же, если обращать внимание только на *сами слагаемые*, они тем не менее, будут различаться, если мы будем принимать во внимание также *порядок расположения* слагаемых; то, что от этого мы получаем пользу, будет достаточно ясно из дальнейшего.

## Представление чисел; определитель

154

*Мы будем говорить, что некоторое число представляется некоторой формой, если неизвестным формы могут быть приданы такие целочисленные значения, при которых значение формы равно заданному числу. При этом имеет место следующая теорема.*

**Теорема.** *Если число  $M$  может быть представлено формой  $(a, b, c)$  так, что значения неизвестных, дающие это представление, взаимно просты, то  $b^2 - ac$  является квадратичным вычетом числа  $M$ .*

**Доказательство.** Если значения неизвестных суть  $m, n$ , так что

$$am^2 + 2bmn + cn^2 = M,$$

и два числа  $\mu, \nu$  подобраны так, что  $\mu t + \nu n = 1$  (п. 40), то, как легко показать, раскрывая скобки,

$$\begin{aligned} (at^2 + 2b\mu n + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2) = \\ = [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac)(m\mu + n\nu)^2, \end{aligned}$$

или

$$M(a\nu^2 - 2b\mu\nu + c\mu^2) = [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac).$$

Поэтому

$$b^2 - ac \equiv [\mu(mb + nc) - \nu(ma + nb)]^2 \pmod{M},$$

т. е.  $b^2 - ac$  есть квадратичный вычет числа  $M$ .

Число  $b^2 - ac$ , от свойств которого, как мы покажем в дальнейшем, в основном зависят свойства формы  $(a, b, c)$ , мы будем называть **определителем этой формы**.

**Значения выражения  $\sqrt{b^2 - ac} \pmod{M}$ ,  
которым принадлежит представление числа  $M$  формой  $(a, b, c)$**

155

Как мы показали,

$$\mu(mb + nc) - \nu(ma + nb)$$

является значением выражения

$$\sqrt{b^2 - ac} \pmod{M}.$$

Однако, как известно, числа  $\mu, \nu$ , для которых  $\mu t + \nu n = 1$ , могут выбираться бесчисленным множеством способов, так что будут получаться все новые и новые значения указанного выражения. Посмотрим, в какой связи они находятся между собой. Пусть не только  $\mu t + \nu n = 1$ , но и  $\mu' t + \nu' n = 1$ ; положим

$$\mu(mb + nc) - \nu(ma + nb) = v, \quad \mu'(mb + nc) - \nu'(ma + nb) = v'.$$



Если из равенства  $\mu t + \nu n = 1$ , умноженного на  $\mu'$ , вычесть равенство  $\mu' t + \nu' n = 1$ , умноженное на  $\mu$ , то получится  $\mu' - \mu = n(\mu' \nu - \mu \nu')$ ; точно так же, умножая первое равенство на  $\nu'$ , а второе на  $\nu$  и вычитая, получаем  $\nu' - \nu = t(\mu \nu' - \mu' \nu)$ . Отсюда тотчас же следует

$$\nu - \nu' = (\mu' \nu - \mu \nu') (at^2 + 2btm + cn^2) = (\mu' \nu - \mu \nu') M,$$

или  $\nu \equiv \nu' \pmod{M}$ . Итак, каким бы образом  $\mu$  и  $\nu$  ни выбирались формула  $\mu(tb + nc) - \nu(ta + nb)$  не может давать различных (т. е. несравнимых) значений выражения  $\sqrt{b^2 - ac} \pmod{M}$ . Поэтому, если  $\nu$  есть какое-нибудь значение указанной формулы, то мы будем говорить, что *представление числа  $M$  формой  $ax^2 + 2bxy + cy^2$ , при котором  $x = t$ ,  $y = n$ , принадлежит значению  $\nu$  выражения  $\sqrt{b^2 - ac} \pmod{M}$* . Впрочем, легко показать, что если  $\nu$  есть какое-нибудь значение указанной формулы, и  $\nu \equiv \nu' \pmod{M}$ , то вместо чисел  $\mu, \nu$ , дающих  $\nu$ , можно подобрать другие числа,  $\mu'$  и  $\nu'$ , которые дают  $\nu'$ . Действительно, если положить

$$\mu' = \mu + \frac{n(\nu' - \nu)}{M}, \quad \nu' = \nu - \frac{t(\nu' - \nu)}{M},$$

то будет иметь место

$$\mu' t + \nu' n = \mu t + \nu n = 1,$$

а значение формулы для  $\mu'$  и  $\nu'$  будет превосходить ее значение для  $\mu$  и  $\nu$  на величину  $(\mu' \nu - \mu \nu') M$ , которая равна  $(\mu t + \nu n)(\nu' - \nu) = \nu' - \nu$ , т. е. первое значение будет равно  $\nu'$ .

Если имеется два представления одного и того же числа одной и той же формой  $(a, b, c)$ , при которых неизвестные имеют взаимно простые значения, то они могут принадлежать как одному и тому же значению выражения  $\sqrt{b^2 - ac} \pmod{M}$ , так и различным значениям. Если

$$M = at^2 + 2btm + cn^2 = am'^2 + 2bm'n' + cn'^2,$$

и

$$\mu t + \nu n = 1, \quad \mu' t' + \nu' n' = 1,$$

то ясно, что если

$$\mu(tb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M},$$

то это сравнение будет оставаться справедливым, какие бы другие возможные значения мы ни брали вместо  $\mu, \nu, \mu', \nu'$ ; в этом случае мы будем говорить, что оба представления принадлежат *одному и тому же* значению выражения  $\sqrt{b^2 - ac} \pmod{M}$ . Если же указанное сравнение для каких-нибудь значений  $\mu, \nu, \mu', \nu'$  не выполняется, то оно вообще не будет выполняться ни для каких значений, и представления в этом случае будут принадлежать *различным* значениям. А если

$$\mu(tb + nc) - \nu(ma + nb) \equiv -[\mu'(m'b + n'c) - \nu'(m'a + n'b)],$$

то будем говорить, что представления принадлежат *противоположным* значениям выражения  $\sqrt{b^2 - ac}$ . Все эти термины мы будем использовать также и тогда, когда речь будет идти о нескольких *представлениях одного и того же числа различными формами*, имеющими, однако, одинаковые определители.

**Пример.** Пусть дана форма  $(3, 7, -8)$ , определитель которой равен 73. Мы имеем следующие представления числа 57 этой формой:

$$3 \cdot 13^2 + 14 \cdot 13 \cdot 15 - 8 \cdot 25^2; \quad 3 \cdot 5^2 + 14 \cdot 5 \cdot 9 - 8 \cdot 9^2.$$

Для первого из них можно положить  $\mu = 2, \nu = -1$ , откуда получается значение выражения  $\sqrt{73} \pmod{57}$ , которому принадлежит это представление:

$$2(13 \cdot 7 - 25 \cdot 8) + (13 \cdot 3 + 25 \cdot 7) = -4.$$

Подобным же образом находим, полагая  $\mu = 2, \nu = -1$ , что второе представление принадлежит значению  $+4$ . Следовательно, эти два представления принадлежат *противоположным* значениям.

Прежде чем идти дальше, заметим, что *формы с определителями, равными нулю, при дальнейших исследованиях будут исключены из рассмотрения*, так как они сильно удлиннили бы теоремы, и потому их лучше рассмотреть отдельно.

**Форма, содержащая другую форму или содержащаяся в другой форме; преобразование, собственное и несобственное**

## 157

Если некоторая форма  $F$ , неизвестные которой суть  $x, y$ , может быть переведена в другую форму  $F'$  от неизвестных  $x', y'$  посредством подстановки вида

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

где  $\alpha, \beta, \gamma, \delta$  суть целые числа, то мы будем говорить, что *первая форма содержит вторую, или что вторая содержится в первой*. Если форма  $F$  есть

$$ax^2 + 2bxy + cy^2,$$

а форма  $F'$  есть

$$a'x'^2 + 2b'x'y' + c'y'^2,$$

то мы имеем следующие три равенства:

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$

$$c' = a\beta^2 + 2b\beta\delta + c\delta^2.$$

Если второе равенство умножить само на себя, первое равенство умножить на третье и из первого произведения вычесть второе, то после отбрасывания взаимно уничтожающихся членов получается

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2.$$

Отсюда следует, что определитель формы  $F'$  делится на определитель формы  $F$ , и что частное является квадратом; таким образом, *эти определители имеют одинаковый знак*. Поэтому, если форма  $F'$  в свою очередь может быть подобной подстановкой переведена в форму  $F$ , т. е. как  $F'$  содержится в  $F$ , так и  $F$  содержится в  $F'$ , то определители обеих форм равны между собой\*, а  $(\alpha\delta - \beta\gamma)^2 = 1$ ,

---

\* Из предыдущего анализа вытекает, что эта теорема верна также и для форм, определители которых равны нулю. Однако равенство  $(\alpha\delta - \beta\gamma)^2 = 1$  в этом случае уже не обязательно.

В этом случае мы будем называть формы эквивалентными. Итак, необходимым условием эквивалентности форм является равенство их определителей, хотя из одного этого условия эквивалентность еще не вытекает. Подстановку  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$  мы будем называть собственным преобразованием, если  $\alpha\delta - \beta\gamma$  является положительным числом, и несобственным, если число  $\alpha\delta - \beta\gamma$  отрицательно; относительно формы  $F'$  мы будем говорить, что она содержится в форме  $F$  собственно или несобственно в зависимости от того, переводится ли  $F$  в  $F'$  собственным или несобственным преобразованием. Если формы  $F$  и  $F'$  эквивалентны, то  $(\alpha\delta - \beta\gamma)^2 = 1$ , и потому, если преобразование собственное, то  $\alpha\delta - \beta\gamma = 1$ , а если несобственное — то  $\alpha\delta - \beta\gamma = -1$ . Если несколько преобразований одновременно являются собственными или одновременно несобственными, то мы будем называть их однотипными, а собственное и несобственное преобразования — неоднотипными.

### Эквивалентность, собственная и несобственная

158

Если определители форм  $F$ ,  $F'$  равны между собой и  $F'$  содержится в  $F$ , то и  $F$  будет содержаться в  $F'$ , причем собственно или несобственно в зависимости от того, собственно или несобственно  $F'$  содержится в  $F$ .

Пусть  $F$  переходит в  $F'$  при подстановке

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'.$$

Тогда  $F'$  будет переходить в  $F$  при подстановке

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y;$$

действительно, при этой подстановке из  $F'$  будет получаться то же, что получается из  $F$ , если положить

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \quad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y),$$

или

$$x = (\alpha\delta - \beta\gamma)x, \quad y = (\alpha\delta - \beta\gamma)y.$$

Но при этом из  $F$  получается, очевидно,  $(\alpha\delta - \beta\gamma)^2 F$ , т. е. снова  $F$  (согласно предыдущему пункту). Очевидно, однако, что последнее преобразование будет собственным или несобственным в зависимости от того, является ли собственным или несобственным первое преобразование.

Если как  $F'$  в  $F$ , так и  $F$  в  $F'$  содержатся собственно, мы будем называть эти формы собственно эквивалентными, а если они содержатся одна в другой несобственно, то — несобственно эквивалентными. В целесообразности такого подразделения мы вскоре убедимся.

**Пример.** Форма  $2x^2 - 8xy + 3y^2$  при подстановке  $x = 2x' + y'$ ,  $y = 3x' + 2y'$  переходит в форму  $-13x'^2 - 12x'y' - 2y'^2$ , а она в свою очередь переходит в первую форму, если положить  $x' = 2x - y$ ,  $y' = -3x + y$ . Следовательно, формы  $(2, -4, 3)$  и  $(-13, -6, -2)$  собственно эквивалентны.

**Проблемы, к рассмотрению которых мы теперь переходим, заключаются в следующем.**

I. Если даны какие-нибудь две формы с одинаковыми определителями, то требуется узнать, эквивалентны ли они или нет; если эквивалентны, то собственно, несобственно или одновременно и собственно и несобственно, так как это тоже возможно. Если же они имеют различные определители, то нужно уметь определить, содержит ли одна из них другую, и если содержит, то собственно, несобственно или одновременно и тем и другим способом. Наконец, нужно найти все, как собственные, так и несобственные, преобразования одной формы в другую.

II. Если дана некоторая форма, то нужно определить, представляется ли ею заданное число и найти все представления. Так как при этом формы с отрицательными определителями требуют при рассмотрении этого вопроса методов, отличных от тех, которые требуются для форм с положительными определителями, то мы сначала укажем все, что является общим для обоих случаев, а только после этого станем рассматривать формы каждого типа в отдельности.

## Противоположные формы

159

*Если форма  $F$  содержит форму  $F'$ , которая в свою очередь содержит форму  $F''$ , то форма  $F$  содержит и форму  $F''$ .*

Пусть неизвестные, от которых соответственно зависят формы  $F, F', F''$  суть  $x, y; x', y'; x'', y''$ , и  $F$  переходит в  $F'$  при подстановке

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

а  $F'$  переходит в  $F''$  при подстановке

$$x' = \alpha' x'' + \beta' y'', \quad y' = \gamma' x'' + \delta' y''.$$

Тогда  $F$  будет, очевидно, переводиться в  $F''$  подстановкой

$$x = \alpha (\alpha' x'' + \beta' y'') + \beta (\gamma' x'' + \delta' y''), \quad y = \gamma (\alpha' x'' + \beta' y'') + \delta (\gamma' x'' + \delta' y'')$$

или

$$x = (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y'', \quad y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''.$$

Следовательно,  $F$  будет также содержать форму  $F''$ .

Так как разность  $(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma')$  равна  $(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$  и потому положительна, если числа  $\alpha\delta - \beta\gamma$  и  $\alpha'\delta' - \beta'\gamma'$  либо оба положительны, либо оба отрицательны, и отрицательна, если одно из этих чисел положительно, а другое отрицательно, то форма  $F$  содержит форму  $F''$  *собственно или несобственно* в зависимости от того, содержат ли форма  $F$  форму  $F'$  и форма  $F'$  форму  $F''$  одинаковым или неодинаковым образом.

Отсюда следует, что если имеется любое количество форм  $F, F', F'', F''', \dots$ , каждая из которых содержит следующую, то первая форма содержит последнюю, причем собственно, если число форм, содержащих следующую за ней несобственно, четно, и несобственно если это число нечетно.

*Если форма  $F$  эквивалентна форме  $F'$ , а  $F'$  в свою очередь эквивалентна форме  $F''$ , то форма  $F$  эквивалентна форме  $F''$ , причем — собственно, если эквивалентности формы  $F$  форме  $F'$  и формы  $F'$  форме  $F''$  одного типа, и — несобственно, если эти эквивалентности различных типов.*

Действительно, так как формы  $F$ ,  $F'$  эквивалентны соответственно формам  $F'$ ,  $F''$ , то не только первые из них соответственно содержат вторые (откуда следует, что  $F$  содержит также и  $F''$ ), но и вторые содержат первые. Поэтому  $F$  и  $F''$  эквивалентны. Из предыдущего же следует, что  $F$  содержит форму  $F''$  собственно или несобственно в зависимости от того, эквивалентны ли форма  $F$  форме  $F'$  и форма  $F'$  форме  $F''$  одинаковым или неодинаковым образом; так же и форма  $F''$  содержит форму  $F$ . Поэтому формы  $F$  и  $F''$  будут эквивалентны, в первом случае собственно, а во втором несобственно.

Формы  $(a, -b, c)$ ,  $(c, b, a)$ ,  $(c, -b, a)$  эквивалентны форме  $(a, b, c)$ , причем первые две — несобственно, а третья — собственно.

Действительно,  $ax^2 + 2bxy + cy^2$  переходит в  $ax'^2 - 2bx'y' + cy'^2$ , если положить  $x = x' + 0 \cdot y'$ ,  $y = 0 \cdot x' - y'$ , причем это преобразование несобственное, так как  $1 \cdot (-1) - 0 \cdot 0 = -1$ . В форму же  $cx'^2 + 2bx'y' + ay'^2$  первая форма переходит посредством несобственного преобразования  $x = 0 \cdot x' + y'$ ,  $y = x' + 0 \cdot y'$ , а в форму  $cx'^2 - 2bx'y' + ay'^2$  при собственном преобразовании  $x = 0 \cdot x' - y'$ ,  $y = x' + 0 \cdot y'$ .

Из этого ясно также и то, что каждая форма, эквивалентная форме  $(a, b, c)$ , собственно эквивалентна либо этой форме, либо форме  $(a, -b, c)$ , а также, что если некоторая форма содержит форму  $(a, b, c)$  или содержится в ней, то она собственно содержит форму  $(a, b, c)$  или форму  $(a, -b, c)$ , или же собственно содержится в одной из них. Формы  $(a, b, c)$  и  $(a, -b, c)$  мы будем называть противоположными.

### Соседние формы

160

Если формы  $(a, b, c)$  и  $(a', b', c')$  имеют одинаковые определители, и, кроме того,  $c = a'$  и  $b \equiv -b' \pmod{c}$  или  $b + b' \equiv 0 \pmod{c}$ , то мы будем называть эти формы соседними, причем в тех случаях, когда будет нужна бóльшая точность, мы будем называть первую форму соседней для второй слева, а вторую — соседней для первой справа.

Так, например, форма  $(7, 3, 2)$  является соседней справа для

формы  $(3, 4, 7)$ , а форма  $(3, 1, 3)$  — соседняя своей противоположной форме  $(3, -1, 3)$  с обеих сторон.

*Соседние формы всегда собственно эквивалентны.* Действительно, форма  $ax^2 + 2bxy + cy^2$  переходит в соседнюю форму  $sx'^2 + 2b'x'y' + c'y'^2$  при подстановке  $x = -y'$ ,  $y = x' + \frac{b+b'}{c} \cdot y'$  (которая является собственной, ибо  $0 \cdot \frac{b+b'}{c} - 1(-1) = 1$ ), что легко доказывается выкладкой с использованием равенства  $b^2 - ac = b'^2 - a'c'$ ; число же  $(b+b')/c$  по предположению является целым. Впрочем, эти пояснения и следствия не имеют силы, если  $c = a' = 0$ . Но этот случай может представиться только для форм, определители которых являются квадратами.

Формы  $(a, b, c)$  и  $(a', b', c')$  собственно эквивалентны, если  $a = a'$ ,  $b \equiv b' \pmod{a}$ . Действительно, форма  $(a, b, c)$  (согласно предыдущему пункту) собственно эквивалентна форме  $(c, -b, a)$ , а последняя является соседней слева для формы  $(a', b', c')$ .

## Общие делители коэффициентов форм

161

*Если форма  $(a, b, c)$  содержит форму  $(a', b', c')$ , то каждый общий делитель чисел  $a, b, c$  является также и общим делителем чисел  $a', b', c'$ , а каждый общий делитель чисел  $a, 2b, c$  — общим делителем чисел  $a', 2b', c'$ .*

Именно, если форма  $ax^2 + 2bxy + cy^2$  переводится в форму  $a'x'^2 + 2b'x'y' + c'y'^2$  подстановкой  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$ , то выполняются следующие равенства:

$$\begin{aligned} a\alpha^2 + 2b\alpha\gamma + c\gamma^2 &= a', \\ a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta &= b', \\ a\beta^2 + 2b\beta\delta + c\delta^2 &= c', \end{aligned}$$

из которых теорема следует тотчас же, если для доказательства ее второй части вместо второго равенства использовать равенство

$$2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'.$$



Из этого вытекает, что наибольший общий делитель чисел  $a, b(2b), c$  входит в наибольший общий делитель чисел  $a', b'(2b'), c'$ . Если же, кроме того, и форма  $(a', b', c')$  содержит форму  $(a, b, c)$ , т. е. если эти формы эквивалентны, то наибольшие общие делители чисел  $a, b(2b), c$  и  $a', b'(2b'), c'$  будут равны, так как каждый из них должен входить в другой. Поэтому, если в этом случае числа  $a, b(2b), c$  не имеют общих делителей, т. е. их наибольший общий делитель равен 1, то и числа  $a', b'(2b'), c'$  не будут обладать общими делителями.

### Связь между всевозможными однотипными преобразованиями одной заданной формы в другую

162

**Задача.** Пусть форма

$$F = AX^2 + 2BXY + CY^2$$

содержит форму

$$f = ax^2 + 2bxy + cy^2,$$

и дано некоторое преобразование первой формы во вторую; найти все остальные однотипные с ним преобразования.

**Решение.** Пусть задано следующее преобразование:  $X = \alpha x + \beta y$ ,  $Y = \gamma x + \delta y$ ; предположим сначала, что имеется и некоторое другое преобразование  $X = \alpha'x + \beta'y$ ,  $Y = \gamma'x + \delta'y$ , однотипное с первым, и посмотрим, что из этого будет следовать. Если принять, что определители форм  $F, f$  суть  $D, d$ , и  $\alpha\delta - \beta\gamma = e$ ,  $\alpha'\delta' - \beta'\gamma' = e'$ , то (в силу п. 157)  $d = De^2 = De'^2$ , и так как величины  $e$  и  $e'$ , по условию задачи, должны быть одного знака,  $e = e'$ . Но мы имеем следующие шесть равенств:

$$[1] \quad A\alpha^2 + 2B\alpha\gamma + C\gamma^2 = a,$$

$$[2] \quad A\alpha'^2 + 2B\alpha'\gamma' + C\gamma'^2 = a,$$

$$[3] \quad A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = b,$$

$$[4] \quad A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' = b,$$

$$[5] \quad A\beta^2 + 2B\beta\delta + C\delta^2 = c,$$

$$[6] \quad A\beta'^2 + 2B\beta'\delta' + C\delta'^2 = c.$$

Если для краткости обозначить числа

$$\begin{aligned} & A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma', \\ & A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma'), \\ & A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta' \end{aligned}$$

через  $a'$ ,  $2b'$ ,  $c'$ , то из предшествующих равенств выводятся следующие\*:

$$[7] \quad a'^2 - D(\alpha\gamma' - \gamma\alpha')^2 = a^2,$$

$$[8] \quad \begin{aligned} 2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') &= 2ab, \\ 4b'^2 - D[(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee'] &= 2b^2 + 2ac, \end{aligned}$$

откуда, прибавляя  $2Dee' = 2d = 2b^2 - 2ac$ , мы получаем

$$[9] \quad \begin{aligned} 4b'^2 - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 &= 4b^2, \\ a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') &= b^2, \end{aligned}$$

а из этих равенств, вычитая из них  $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = b^2 - ac$ , мы приходим к равенствам

$$[10] \quad a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac,$$

$$[11] \quad 2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc,$$

$$[12] \quad c'^2 - D(\beta\delta' - \delta\beta')^2 = c^2.$$

Предположим теперь, что наибольший общий делитель чисел  $a$ ,  $2b$ ,  $c$  равен  $m$ , а числа  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$  определены так, что

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = m$$

---

\* Они получаются следующим образом: [7] получается из [1]·[2] (т. е. если мы перемножим равенства [1] и [2], или, точнее, умножим левую часть первого на левую часть второго и правую часть первого на правую часть второго и приравняем произведения), [8] получается из [1]·[4] + [2]·[3], следующее (непронумерованное) равенство из [1]·[6] + [2]·[5] + [3]·[4] + [3]·[4]; непронумерованное равенство, идущее после [9] — из [3]·[4], равенство [11] — из [3]·[6] + [4]·[5], равенство [12] — из [5]·[6]. Обозначений, подобных использованным здесь, мы будем все время придерживаться и в дальнейшем. Выкладки же мы должны предоставить читателю.

(п. 40); умножим тогда равенства [7], [8], [9], [10], [11], [12] соответственно на  $\mathfrak{A}^2$ ,  $2\mathfrak{A}\mathfrak{B}$ ,  $\mathfrak{B}^2$ ,  $2\mathfrak{A}\mathfrak{C}$ ,  $2\mathfrak{B}\mathfrak{C}$ ,  $\mathfrak{C}^2$  и сложим произведения. Если еще для краткости положить

$$[13] \quad \mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T,$$

$$[14] \quad \mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') + \mathfrak{C}(\beta\delta' - \delta\beta') = U,$$

где  $T$  и  $U$ , очевидно, являются целыми числами, то мы получим равенство

$$T^2 - DU^2 = m^2.$$

Мы приходим, таким образом, к следующему изящному заключению: *из любых двух однотипных преобразований формы  $F$  в  $f$  получается решение в целых числах неопределенного уравнения  $t^2 - Du^2 = m^2$ , именно,  $t = T$ ,  $u = U$ .* Так как при наших рассуждениях мы не предполагали, что преобразования различны, то и одно преобразование, примененное дважды, дает решение этого уравнения. При этом, однако, вследствие того, что  $\alpha' = \alpha$ ,  $\beta' = \beta$ , также и  $a' = a$ ,  $b' = b$ ,  $c' = c$ , и, следовательно, получается решение  $T = m$ ,  $U = 0$ , очевидное и непосредственно.

Теперь мы предположим известными первое преобразование и решение неопределенного уравнения и посмотрим, что можно из этого вывести относительно второго преобразования, т. е. каким образом  $\alpha'$ ,  $\beta'$ ,  $\gamma'$ ,  $\delta'$  зависят от  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$ ,  $T$ ,  $U$ . Для этой цели умножим сначала равенство [1] на  $\delta\alpha' - \beta\gamma'$ , равенство [2] — на  $\alpha\delta' - \gamma\beta'$ , равенство [3] — на  $\alpha\gamma' - \gamma\alpha'$ , равенство [4] — на  $\gamma\alpha' - \alpha\gamma'$  и сложим произведения. При этом получается равенство

$$[15] \quad (e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a.$$

Аналогично из

$$(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] - [6])$$

получается равенство

$$[16] \quad 2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b.$$

Наконец, из

$$(\delta\beta' - \beta\delta')([3] - [4]) + (\alpha\delta' - \gamma\beta')[5] + (\delta\alpha' - \beta\gamma')[6]$$

вытекает равенство

$$[17] \quad (e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c.$$

Если значения [15], [16], [17] подставить в [13], то мы получим

$$(e + e') T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') (\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c),$$

или

$$[18] \quad 2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') m,$$

откуда  $T$  может быть выведено много легче, чем из [13]. Если это равенство связать с [15], [16], [17], то получается  $ma' = Ta$ ,  $2mb' = 2Tb$ ,  $mc' = Tc$ . При подстановке этих значений  $a'$ ,  $2b'$ ,  $c'$  в равенства [7]—[12] и замене  $T^2$  на  $m^2 + DU^2$  указанные равенства после соответствующих преобразований переходят в следующие:

$$(\alpha\gamma' - \gamma\alpha')^2 m^2 = a^2 U^2,$$

$$(\alpha\gamma' - \gamma\alpha') (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') m^2 = 2abU^2,$$

$$(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 m^2 = 4b^2 U^2,$$

$$(\alpha\gamma' - \delta\alpha') (\beta\delta' - \delta\beta') m^2 = acU^2,$$

$$(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') (\beta\delta' - \delta\beta') m^2 = 2bcU^2,$$

$$(\beta\delta' - \delta\beta')^2 m^2 = c^2 U^2.$$

Отсюда при помощи равенства [14] и равенства  $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$  легко выводятся (если умножить соответственно на  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$  сначала первое, второе и четвертое равенства, затем второе, третье и пятое и, наконец, четвертое, пятое и шестое и полученные произведения сложить) соотношения

$$(\alpha\gamma' - \gamma\alpha') Um^2 = maU^2,$$

$$(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') Um^2 = 2mbU^2,$$

$$(\beta\delta' - \delta\beta') Um^2 = mcU^2,$$

из которых при делении на  $mU^*$  получается

$$[19] \quad aU = (\alpha\gamma' - \gamma\alpha') m,$$

$$[20] \quad 2bU = (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') m,$$

$$[21] \quad cU = (\beta\delta' - \delta\beta') m;$$

---

\* Этого нельзя было бы делать, если бы  $U$  было равно 0; но в этом случае справедливость равенств [19], [20], [21] тотчас же получалась бы из первого, третьего и шестого равенств.

из любого из этих равенств  $U$  может быть получено намного легче, чем из [14]. Одновременно отсюда следует, что как бы ни были определены  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$  (что можно сделать бесконечным числом способов), значения  $T$  и  $U$  будут сохраняться одними и теми же.

Если теперь умножить равенство [18] на  $\alpha$ , [19] — на  $2\beta$ , [20] — на  $-\alpha$ , то при сложении получается

$$2\alpha eT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha'm = 2e\alpha'm.$$

Аналогичным образом из  $\beta \cdot [18] + \beta \cdot [20] - 2\alpha \cdot [21]$  получается

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta'm = 2e\beta'm.$$

Далее, из  $\gamma \cdot [18] + 2\delta \cdot [19] - \gamma \cdot [20]$  имеем

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma'm = 2e\gamma'm.$$

Наконец, из  $\delta \cdot [18] + \delta \cdot [20] - 2\gamma \cdot [21]$  получается

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta'm = 2e\delta'm.$$

Если в эти формулы подставить вместо  $a, b, c$  их значения из [1], [3], [5], то формулы переходят в следующие:

$$\alpha'm = \alpha T - (\alpha B + \gamma C)U,$$

$$\beta'm = \beta T - (\beta B + \delta C)U,$$

$$\gamma'm = \gamma T - (\alpha A + \gamma B)U,$$

$$\delta'm = \delta T + (\beta A + \delta B)U^*,$$

Из вышеизложенного исследования вытекает, что не существует преобразования формы  $F$  в  $f$ , однотипного с заданным, которое не содержалось бы в формулах

$$(I) \quad \begin{cases} X = \frac{1}{m} [\alpha t - (\alpha B + \gamma C)u]x + \frac{1}{m} [\beta t - (\beta B + \delta C)u]y, \\ Y = \frac{1}{m} [\gamma t + (\alpha A + \gamma B)u]x + \frac{1}{m} [\delta t + (\beta A + \delta B)u]y, \end{cases}$$

где  $t$  и  $u$  обозначают произвольные целые числа, удовлетворяющие уравнению  $t^2 - Du^2 = m^2$ . Однако из этого еще нельзя заключить, что любые значения  $t$  и  $u$ , удовлетворяющие указанному

\* Отсюда легко видеть, что

$$AeU = (\delta\gamma' - \gamma\delta')m, \quad 2BeU = (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m, \quad CeU = (\beta\alpha' - \alpha\beta')m.$$

уравнению, при подстановке в формулы (I) дают требуемые преобразования. Но при помощи равенств [1], [3], [5] и равенства  $t^2 - Du^2 = m^2$  легко устанавливается следующее.

1. Форма  $F$  может быть преобразована в форму  $f$  подстановкой, получающейся из любых значений  $t$  и  $u$ . Выкладки, которые скорее громоздки, чем трудны, мы для краткости опустим.

2. Каждое преобразование, полученное по формулам (I), относительно с заданным. Действительно,

$$\begin{aligned} \frac{1}{m} [\alpha t - (\alpha B + \gamma C) u] \cdot \frac{1}{m} [\delta t + (\beta A + \delta B) u] - \\ - \frac{1}{m} [\beta t - (\beta B + \delta C) u] \cdot \frac{1}{m} [\gamma t + (\alpha A + \gamma B) u] = \\ = \frac{1}{m^2} (\alpha \delta - \beta \gamma) (t^2 - Du^2) = \alpha \delta - \beta \gamma. \end{aligned}$$

3. Если формы  $F$  и  $f$  имеют разные определители, то может случиться, что при некоторых значениях  $t$  и  $u$  формулы (I) будут давать подстановки, которые содержат дроби и потому должны быть отброшены. Все же остальные будут годиться и ими будут исчерпываться все искомые преобразования.

4. Если же формы  $F$  и  $f$  имеют одинаковые определители и потому эквивалентны, то формулы (I) не дают никаких преобразований, содержащих дроби, и потому представляют полное решение задачи для этого случая. Доказывается это следующим образом.

Из теорем предыдущего пункта следует, что в этом случае  $m$  одновременно является общим делителем чисел  $A$ ,  $2B$ ,  $C$ . Так как  $t^2 - Du^2 = m^2$ , то  $t^2 - B^2u^2 = m^2 - ACu^2$ ; таким образом  $t^2 - B^2u^2$  и тем более  $4t^2 - 4B^2u^2$  делится на  $m^2$ , откуда вытекает (ибо  $2B$  делится на  $m$ ), что  $4t^2$  делится на  $m^2$  и, следовательно,  $2t$  делится на  $m$ . Поэтому числа  $2(t + Bu)/m$  и  $2(t - Bu)/m$  являются целыми, и притом (так как их разность  $4Bu/m$  четна) либо одновременно четными, либо одновременно нечетными. Если бы они оба были нечетными, то и их произведение должно было бы быть нечетным; но произведение, будучи равным учетверенному числу  $(t^2 - B^2u^2)/m^2$ , которое, как мы показали выше, целое, обязательно четно. Следовательно, этот случай невозможен; поэтому  $2(t + Bu)/m$  и  $2(t - Bu)/m$  всегда четны, а значит  $(t + Bu)/m$  и  $(t - Bu)/m$  —

всегда числа целые. Из этого уже без труда выводится, что все четыре коэффициента в (I) всегда являются целыми числами.

Из сказанного вытекает, что если известны все решения уравнения  $t^2 - Du^2 = m^2$ , то из этого могут быть выведены все преобразования формы  $(A, B, C)$  в форму  $(a, b, c)$ , однотипные с заданным преобразованием. Как находить решения указанного уравнения, мы покажем позднее. Сейчас заметим только, что количество решений конечно, если  $D$  отрицательно или если  $D$  положительно и притом является квадратом, и бесконечно, если  $D$  — положительное число, не являющееся квадратом. Если имеет место этот последний случай и одновременно  $D$  не равно  $d$  (см. выше случай 3), то нужно было бы еще исследовать, каким образом сразу отличать те значения  $t, u$ , которые дают подстановки, не содержащие дробей, от значений, приводящих к дробным подстановкам. Однако ниже мы изложим для этого случая другой метод, который будет свободен от этого неудобства (п. 214).

Пример. Форма  $x^2 + 2y^2$  при собственной подстановке  $x = 2x' + 7y', y = x' + 5y'$  переходит в форму (6, 24, 99); найдем все собственные преобразования первой формы во вторую. Здесь  $D = -2, m = 3$ , и потому уравнение, которое надлежит решить, есть  $t^2 + 2u^2 = 9$ . Оно удовлетворяется шестью различными способами, именно, при  $t = 3, -3, 1, -1, 1, -1$  и соответственно  $u = 0, 0, 2, 2, -2, -2$ . Первое и третье решения дают подстановки с дробными числами и потому должны быть отброшены; из остальных получаются четыре подстановки

$$x = \begin{cases} 2x' + 7y', \\ -2x' - 7y', \\ -2x' - 9y', \\ 2x' + 9y', \end{cases} \quad y = \begin{cases} x' + 5y', \\ -x' - 5y', \\ x' + 3y', \\ -x' - 3y', \end{cases}$$

первая из которых совпадает с заданной.

### Двусторонние формы

Выше мы мимоходом уже упоминали о том, что некоторая форма  $F$  может содержать другую форму  $F'$  одновременно и собственно

и несобственно. Очевидно, что это будет иметь место, если между формами  $F$  и  $F'$  можно поместить еще одну форму  $G$ , обладающую теми свойствами, что  $F$  содержит  $G$ ,  $G$  содержит  $F'$  и  $G$  несобственно эквивалентна самой себе. Действительно, если мы предположим, что  $F$  содержит форму  $G$  собственно (несобственно), то так как  $G$  несобственно содержит  $G$ ,  $F$  будет содержать  $G$  также и несобственно (собственно), т. е. будет содержать как собственно, так и несобственно (п. 159). Таким же способом мы из предположения, что  $G$  содержит  $F'$ , выводим, что  $F$  содержит  $F'$  и собственно и несобственно. То, что формы, несобственно эквивалентные самим себе, существуют, вытекает из рассмотрения совсем простых примеров, именно, форм со средними членами, равными нулю. Такая форма сама себе противоположна (п. 159) и потому несобственно эквивалентна. Более общо, этим свойством обладает каждая форма  $(a, b, c)$ , у которой  $2b$  делится на  $a$ . Именно, форма  $(c, b, a)$  будет для этой формы соседней слева (п. 160) и потому будет ей собственно эквивалентна; форма же  $(c, b, a)$ , согласно п. 159, несобственно эквивалентна форме  $(a, b, c)$ ; таким образом,  $(a, b, c)$  несобственно эквивалентна самой себе. Такие формы  $(a, b, c)$ , у которых  $2b$  делится на  $a$ , мы будем называть двусторонними. Таким образом, имеет место следующая теорема.

*Форма  $F$  будет содержать форму  $F'$  и собственно и несобственно, если имеется двусторонняя форма, содержащаяся в  $F$  и содержащая  $F'$ .*

Однако эту теорему можно и обратить.

**Теорема, касающаяся случая,  
когда одна форма содержится в другой  
одновременно собственно и несобственно**

164

**Теорема.** *Если форма*

$$F = Ax^2 + 2Bxy + Cy^2$$

*содержит другую форму*

$$F' = A'x'^2 + 2B'x'y' + C'y'^2$$



как собственно, так и несобственно, то всегда можно найти двустороннюю форму, которая содержится в форме  $F$  и содержит форму  $F'$ .

Предположим, что форма  $F$  переводится в форму  $F'$  как подстановкой

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

так и неотнотипной с ней подстановкой

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'.$$

Если тогда числа  $\alpha\delta - \beta\gamma$ ,  $\alpha'\delta' - \beta'\gamma'$  обозначить соответственно через  $e$ ,  $e'$ , то  $B'^2 - A'C' = e^2(B^2 - AC) = e'^2(B^2 - AC)$ , откуда  $e^2 = e'^2$ , и, так как, по предположению,  $e$  и  $e'$  имеют противоположные знаки,  $e = -e'$  или  $e + e' = 0$ . Если теперь в  $F'$  положить  $x' = \delta'x'' - \beta'y''$  и  $y' = -\gamma'x'' + \alpha'y''$ , то, очевидно, получится та же самая форма, которая получается из  $F$ , если положить

или

$$\begin{aligned} 1) \quad x &= \alpha(\delta'x'' - \beta'y'') + \beta(-\gamma'x'' + \alpha'y'') = (\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y'', \\ y &= \gamma(\delta'x'' - \beta'y'') + \delta(-\gamma'x'' + \alpha'y'') = (\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y'', \end{aligned}$$

или

$$\begin{aligned} 2) \quad x &= \alpha'(\delta'x'' - \beta'y'') + \beta'(-\gamma'x'' + \alpha'y'') = e'x'', \\ y &= \gamma'(\delta'x'' - \beta'y'') + \delta'(-\gamma'x'' + \alpha'y'') = e'y''. \end{aligned}$$

Поэтому, если числа  $\alpha\delta' - \beta\gamma'$ ,  $\beta\alpha' - \alpha\beta'$ ,  $\gamma\delta' - \delta\gamma'$ ,  $\delta\alpha' - \gamma\beta'$  обозначить соответственно через  $a$ ,  $b$ ,  $c$ ,  $d$ , то форма  $F$  обеими подстановками

$$x = ax'' + by'', \quad y = cx'' + dy''; \quad x = e'x'', \quad y = e'y''$$

будет переводиться в одну и ту же форму, откуда получаются следующие три равенства:

$$[1] \quad Aa^2 + 2Bac + Cc^2 = Ae'^2,$$

$$[2] \quad Aab + B(ad + bc) + Ccd = Be'^2,$$

$$[3] \quad Ab^2 + 2Bbd + Cd^2 = Ce'^2.$$

Из значений же чисел  $a$ ,  $b$ ,  $c$ ,  $d$  находим

$$[4] \quad ad - bc = ee' = -e^2 = -e'^2.$$

Поэтому из  $d \cdot [1] - c \cdot [2]$  получается

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'^2,$$

и потому

$$A(a + d) = 0.$$

Далее, из  $(a + d) \cdot [2] - b \cdot [1] - c \cdot [3]$  вытекает

$$[Ab + B(a + d) + Cc](ad - bc) = [-Ab + B(a + d) - Cc]e'^2,$$

и потому

$$B(a + d) = 0.$$

Наконец, из  $a \cdot [3] - b \cdot [2]$  имеем

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)e'^2,$$

и потому

$$C(a + d) = 0.$$

Так как все три величины  $A, B, C$  не могут быть одновременно равными нулю, мы получаем  $a + d = 0$  или  $a = -d$ .

Из  $a \cdot [2] - b \cdot [1]$  следует

$$(Ba + Cc)(ad - bc) = (Ba - Ab)e'^2,$$

откуда

$$[5] \quad Ab - 2Ba - Cc = 0.$$

Из равенств  $e + e' = 0, a + d = 0$ , или

$$\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma' = 0, \quad \alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha' = 0,$$

следует  $(\alpha + \alpha')(\delta + \delta') = (\beta + \beta')(\gamma + \gamma')$ , или

$$(\alpha + \alpha') : (\gamma + \gamma') = (\beta + \beta') : (\delta + \delta').$$

Пусть это отношение, выраженное в наименьших числах, имеет вид  $m : n$ , так что  $m$  и  $n$  взаимно просты\*; возьмем такие числа

---

\* Если бы все величины  $\alpha + \alpha', \gamma + \gamma', \beta + \beta', \delta + \delta'$  были равны нулю, то соотношение было бы неопределенным, и потому такой метод был бы неприменим. Но при некоторой внимательности можно заметить, что это при

$\mu, \nu$ , что  $\mu t + \nu n = 1$ . Далее, пусть  $r$  есть наибольший общий делитель чисел  $a, b, c$ , квадрат которого будет, следовательно, входить также в  $a^2 + bc$  или  $bc - ad$ , или  $e^2$ , так что  $r$  является также и делителем  $e$ . Если теперь форму, в которую переходит форма  $F$  при подстановке

$$x = mt + \frac{\nu e}{r} u, \quad y = nt - \frac{\mu e}{r} u,$$

обозначить через  $G = Mt^2 + 2Ntu + Pu^2$ , то  $G$  будет двусторонней и будет содержать форму  $F'$ .

**Доказательство, I.** Чтобы сделать ясным, что форма  $G$  — двусторонняя, мы покажем, что

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr,$$

откуда, так как  $r$  входит в  $a, b, c$ , будет следовать, что число  $(b\mu^2 - 2a\mu\nu - c\nu^2)/r$  целое, и потому  $2N$  есть кратность числа  $M$ . Но

$$[6] \quad M = Am^2 + 2Bmn + Cn^2, \quad Nr = [Am\nu - B(m\mu - n\nu) - Cn\mu]e.$$

Далее, раскрывая скобки, легко установить, что

$$2e + 2a = e - e' + a - d = (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma'),$$

$$2b = (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta').$$

Отсюда следует, так как  $m(\gamma + \gamma') = n(\alpha + \alpha')$   $m(\delta + \delta') = n(\beta + \beta')$ , что  $m(2e + 2a) = -2nb$  или

$$[7] \quad me + ma + nb = 0.$$

Аналогично,

$$2e - 2a = e - e' - a + d = (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma'),$$

$$2c = (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta'),$$

и отсюда следует  $n(2e - 2a) = -2mc$ , или

$$[8] \quad ne - na + mc = 0.$$

наших предположениях невозможно. Действительно, тогда имело бы место  $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$ , т. е.  $e = e'$ , и потому, в силу  $e = -e'$ , было бы  $e = e' = 0$ . Отсюда следовало бы, что и  $B'^2 - A'C' = 0$ , т. е. определитель формы  $F'$  равен 0, однако такие формы мы раз и навсегда исключили из рассмотрения.

Если теперь к  $m^2(b\mu^2 - 2a\mu\nu - c\nu^2)$  прибавить выражение

$$(1 - t\mu - n\nu)[t\nu(e - a) + (t\mu + 1)b] + (te + ta + nb)(t\mu\nu + \nu) + \\ + (ne - na + tc)t\nu^2,$$

которое вследствие

$$1 - t\mu - n\nu = 0, \quad te + ta + nb = 0, \quad ne - na + tc = 0,$$

очевидно, равно нулю, то после раскрытия скобок и отбрасывания взаимно уничтожающихся членов мы получим  $2t\nu e + b$ . Поэтому

$$[9] \quad m^2(b\mu^2 - 2a\mu\nu - c\nu^2) = 2t\nu e + b.$$

Прибавляя аналогичным образом к  $mn(b\mu^2 - 2a\mu\nu - c\nu^2)$  выражение

$$(1 - t\mu - n\nu)[(n\nu - t\mu)e - (1 + t\mu + n\nu)a] - (te + ta + nb)t\mu^2 + \\ + (ne - na + tc)n\nu^2,$$

находим

$$[10] \quad mn(b\mu^2 - 2a\mu\nu - c\nu^2) = (n\nu - t\mu)e - a.$$

Наконец, если к  $n^2(b\mu^2 - 2a\mu\nu - c\nu^2)$  прибавить выражение

$$(t\mu + n\nu - 1)[n\mu(e + a) + (\nu n + 1)c] - (te + ta + nb)n\mu^2 - \\ - (ne - na + tc)(n\mu\nu + \mu),$$

то получится

$$[11] \quad n^2(b\mu^2 - 2a\mu\nu - c\nu^2) = -2n\mu e - c.$$

Теперь из [9], [10], [11] получается

$$(Am^2 + 2Bmn + Cn^2)(b\mu^2 - 2a\mu\nu - c\nu^2) = \\ = 2e[At\nu + B(n\nu - t\mu) - Cn\mu] + Ab - 2Ba - Cc$$

или, в силу [6],

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr.$$

II. Чтобы доказать, что форма  $G$  содержит форму  $F'$ , мы покажем, что, во-первых,  $G$  переходит в  $F'$ , если положить

$$(S)t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y', \quad u = \frac{r}{e}(n\alpha - t\gamma)x' + \frac{r}{e}(n\beta - t\delta)y',$$

и, во-вторых, что  $r(n\alpha - m\gamma)/e$  и  $r(n\beta - m\delta)/e$  суть целые числа.

1. Так как  $F$  переходит в  $G$ , если положить

$$x = mt + \frac{\nu e}{r} u, \quad y = nt - \frac{\mu e}{r} u,$$

то  $G$  преобразуется подстановкой  $(S)$  в ту же самую форму, в которую преобразуется  $F$ , если положить

$$\begin{aligned} x &= m[(\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'] + \nu[(n\alpha - m\gamma)x' + (n\beta - m\delta)y'] = \\ &= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y' = \alpha x' + \beta y', \end{aligned}$$

$$\begin{aligned} y &= n[(\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'] - \mu[(n\alpha - m\gamma)x' + (n\beta - m\delta)y'] = \\ &= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y' = \gamma x' + \delta y'. \end{aligned}$$

Но этой подстановкой  $F$  переводится в  $F'$ ; поэтому и  $G$  подстановкой  $(S)$  будет переводиться в  $F'$ .

2. Из значений  $e, b, d$  находим, что  $\alpha'e + \gamma b - \alpha d = 0$ , или, вследствие того, что  $d = -a$ ,  $n\alpha'e + n\alpha a + n\gamma b = 0$ . Отсюда в силу [7],  $n\alpha'e + n\alpha a = m\gamma e + m\gamma a$ , или

$$[12] \quad (n\alpha - m\gamma)a = (m\gamma - n\alpha')e.$$

Далее,  $\alpha nb = -\alpha m(e + a)$ ,  $\gamma mb = -m(\alpha'e + \alpha a)$ , и потому

$$[13] \quad (n\alpha - m\gamma)b = (\alpha' - \alpha)me.$$

Наконец,  $\gamma'e - \gamma a + \alpha c = 0$ ; если умножить это равенство на  $n$  и подставить вместо  $na$  его значение из [8], то получается

$$[14] \quad (n\alpha - m\gamma)c = (\gamma - \gamma')ne.$$

Аналогичным образом выводится  $\beta'e + \delta b - \beta d = 0$ , или  $n\beta'e + n\delta b + n\beta a = 0$ , и потому, в силу [7],  $n\beta'e + n\beta a = m\delta e + m\delta a$  или

$$[15] \quad (n\beta - m\delta)a = (m\delta - n\beta')e.$$

Далее,  $\beta nb = -\beta m(e + a)$ ,  $\delta mb = -m(\beta'e + \beta a)$ , и потому

$$[16] \quad (n\beta - m\delta)b = (\beta' - \beta)me.$$

Наконец,  $\delta'e - \delta a + \beta c = 0$ ; если умножить это равенство на  $n$  и подставить вместо  $na$  его значение из [8], то получается

$$[17] \quad (n\beta - m\delta)c = (\delta - \delta')ne.$$

Так как наибольший общий делитель чисел  $a, b, c$  равен  $r$ , то можно теперь найти такие целые числа  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ , что

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r.$$

Если эти числа найдены, то из [12], [13], [14]; [15], [16], [17] следует

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \frac{r}{e}(n\alpha - m\gamma),$$

$$\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n = \frac{r}{e}(n\beta - m\delta),$$

и потому числа  $r(n\alpha - m\gamma)/e$  и  $r(n\beta - m\delta)/e$  — целые.

### 165

**Пример.** Форма  $3x^2 + 14xy - 4y^2$  преобразуется в форму  $-12x'^2 - 18x'y' + 39y'^2$  как собственно, если положить

$$x = 4x' + 11y', \quad y = 15x' - 18y',$$

так и несобственно, если положить

$$x = -74x' + 89y', \quad y = 15x' - 18y'.$$

Числа  $\alpha + \alpha', \beta + \beta', \gamma + \gamma', \delta + \delta'$  равны здесь соответственно  $-70, 100, 14, -20$ . При этом  $-70 : 14 = 100 : -20 = 5 : -1$ . Мы полагаем поэтому  $m = 5, n = -1, \mu = 0, \nu = -1$ . В качестве чисел  $a, b, c$  находим  $-237, -1170, 48$ , наибольший общий делитель которых  $r$  равен 3. Наконец,  $e = 3$ . Поэтому преобразование  $x = 5t - u, y = -t$  переводит форму  $(3, 7, -4)$  в двустороннюю форму  $t^2 - 16tu + 3u^2$ .

Если формы  $F, F'$  эквивалентны, то форма  $G$ , содержась в  $F$ , будет содержаться также и в  $F'$ . Но так как  $G$  в свою очередь содержит  $F'$ ,  $G$  будет эквивалентна  $F'$ , а, следовательно, эквива-

лентна также и форме  $F$ . Таким образом, в этом случае теорема может быть высказана в следующем виде.

*Если формы  $F$  и  $F'$  эквивалентны как собственно, так и несобственно, то можно найти двустороннюю форму, эквивалентную обоим этим формам.*

Между прочим, в этом случае  $e = \pm 1$ , а потому и  $r$ , которое входит в  $e$ , равно 1.

В отношении преобразований форм мы удовольствуемся изложенным и перейдем теперь к рассмотрению вопроса о представлениях чисел.

### Общее исследование о представлениях чисел формами и о связи этих представлений с преобразованиями

#### 166

*Если форма  $F$  содержит форму  $F'$ , то каждое число, которое может быть представлено формой  $F'$ , может быть также представлено и формой  $F$ .*

Пусть неизвестные форм  $F$ ,  $F'$  суть соответственно  $x, y$ ;  $x', y'$ , и предположим, что число  $M$  представляется формой  $F'$  при  $x' = m$ ,  $y' = n$ , а форма  $F$  переводится в  $F'$  подстановкой

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'.$$

Тогда очевидно, что если мы положим

$$x = \alpha m + \beta n, \quad y = \gamma m + \delta n,$$

форма  $F$  представит  $M$ .

Если  $M$  представляется формой  $F'$  различными способами, например, также и при  $x' = m'$ ,  $y' = n'$ , то отсюда будут получаться и различные представления  $M$  формой  $F$ . Действительно, если бы было  $\alpha m + \beta n = \alpha m' + \beta n'$  и  $\gamma m + \delta n = \gamma m' + \delta n'$ , то имело бы место или  $\alpha\delta - \beta\gamma = 0$ , что противоречит нашему предположению о том, что определитель формы  $F$  не равен нулю, или  $m = m'$ ,  $n = n'$ . Отсюда следует, что  $M$  может быть представлено формой  $F$  по

меньшей мере столькими же различными способами, что и формой  $F'$ .

Поэтому, если как  $F$  содержит форму  $F'$ , так и  $F'$  содержит форму  $F$ , т. е. если  $F$  и  $F'$  эквивалентны, и число  $M$  представляется одной из них, то оно представляется и другой, причем столькими же различными способами, что и первой.

Наконец, заметим, что в этом случае наибольший общий делитель чисел  $m$ ,  $n$  равен наибольшему общему делителю чисел  $\alpha m + \beta n$ ,  $\gamma m + \delta n$ . Если первый равен  $\Delta$ , и числа  $\mu$ ,  $\nu$  подобраны так, что  $\mu m + \nu n = \Delta$ , то

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm \Delta.$$

Поэтому наибольший общий делитель чисел  $\alpha m + \beta n$ ,  $\gamma m + \delta n$  входит также и в  $\Delta$ , а  $\Delta$  в свою очередь входит в него, так как входит в  $\alpha m + \beta n$  и  $\gamma m + \delta n$ . Следовательно, оба наибольших общих делителя равны. В частности, если  $m$ ,  $n$  взаимно просты, то  $\alpha m + \beta n$ ,  $\gamma m + \delta n$  будут взаимно просты.

**Теорема.** Если формы

$$F = ax^2 + 2bxy + cy^2,$$

$$F' = a'x'^2 + 2b'x'y' + c'y'^2$$

эквивалентны, определители их равны  $D$ , вторая форма переводится в первую подстановкой

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y$$

и если, далее, число  $M$  представляется формой  $F$  при  $x = m$ ,  $y = n$  и потому формой  $F'$  — при

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n',$$

причем так, что  $m$  взаимно просто с  $n$ , и потому и  $m'$  взаимно просто с  $n'$ , то оба представления будут принадлежать или одному и тому же, или противоположным значениям выражения  $\sqrt{D} \pmod{M}$  в зависимости от того, является ли преобразование формы  $F'$  в  $F$  собственным или несобственным.



**Доказательство.** Если мы определим числа  $\mu$ ,  $\nu$  так, что  $\mu t + \nu n = 1$ , и положим

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

(эти величины, в силу того, что  $\alpha\delta - \beta\gamma = \pm 1$ , являются целыми числами), то (согласно сказанному в конце предыдущего пункта) будет выполняться равенство

$$\mu' t' + \nu' n' = 1.$$

Если, далее,

$$\mu(bt + cn) - \nu(at + bn) = V, \quad \mu'(b't' + c'n') - \nu'(a't' + b'n') = V',$$

то  $V$ ,  $V'$  будут значениями выражения  $\sqrt{D} \pmod{M}$ , которым принадлежат соответственно первое и второе представления. Подставляя в  $V'$  вместо  $\mu'$ ,  $\nu'$ ,  $t'$ ,  $n'$  их выражения, а в  $V$

вместо  $a$  выражение  $a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2$ ,

вместо  $b$  выражение  $a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$ ,

вместо  $c$  выражение  $a'\beta^2 + 2b'\beta\delta + c'\delta^2$ ,

находим после соответствующих преобразований, что

$$V = V'(\alpha\delta - \beta\gamma).$$

Поэтому или  $V = V'$ , или  $V = -V'$ , в зависимости от того,  $\alpha\delta - \beta\gamma = +1$  или  $= -1$ , т. е. представления будут принадлежать или одному и тому же, или противоположным значениям выражения  $\sqrt{D} \pmod{M}$ , в зависимости от того, будет ли преобразование формы  $F'$  в  $F$  собственным или не собственным.

Поэтому если имеется несколько представлений числа  $M$  формой  $(a, b, c)$  при взаимно простых значениях неизвестных  $x, y$ , которые принадлежат различным значениям выражения  $\sqrt{D} \pmod{M}$ , то соответствующие представления формой  $(a', b', c')$  будут принадлежать тем же самым (противоположным) значениям, а если для одной из форм нет представления числа  $M$ , принадлежащего какому-нибудь определенному значению, то для эквивалентной формы нет представления, принадлежащего этому же (противоположному) значению.

**Теорема.** Если число  $M$  представляется формой  $ax^2 + 2bxy + cy^2$ , когда неизвестным  $x, y$  придаются взаимно простые значения  $m, n$ , и если значение выражения  $\sqrt{D} \pmod{M}$ , которому принадлежит это представление, равно  $N$ , то формы  $(a, b, c)$  и  $(M, N, (N^2 - D)/M)$  собственно эквивалентны.

**Доказательство.** Из п. 155 вытекает, что можно найти целые числа  $\mu, \nu$  с тем свойством, что

$$m\mu + n\nu = 1, \quad \mu(bt + cn) - \nu(at + bn) = N.$$

Если это сделано, то подстановкой  $x = mx' - \nu y'$ ,  $y = nx' + \mu y'$ , которая, очевидно, является собственной, форма  $(a, b, c)$  переводится в форму, определитель которой равен  $D(m\mu + n\nu)^2$ , т. е. равен  $D$ , другими словами, в эквивалентную форму. Если записать эту форму в виде  $(M', N', (N'^2 - D)/M')$ , то

$$M' = at^2 + 2bmn + cn^2 = M, \quad N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N.$$

Поэтому форма, в которую переводится  $(a, b, c)$  указанным преобразованием, представляется в виде  $(M, N, (N^2 - D)/M)$ .

Из равенств

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

следует, между прочим, что

$$\mu = \frac{nN + ma + nb}{at^2 + 2bmn + cn^2} = \frac{nN + ma + nb}{M}, \quad \nu = \frac{mb + nc - mN}{M},$$

и потому стоящие справа выражения являются целыми числами.

Заметим еще, что эта теорема неверна, если  $M = 0$ , так как тогда член  $(N^2 - D)/M$  будет неопределенным\*.

Если имеется несколько представлений числа  $M$  формой  $(a, b, c)$ , принадлежащих одному и тому же значению  $N$  выражения

---

\* Если мы захотим применять нашу терминологию также и в этом случае, то выражение « $N$  есть значение выражения  $\sqrt{D} \pmod{M}$ », или  $N^2 \equiv D \pmod{M}$ », должно означать, что число  $N^2 - D$  есть кратность числа  $M$  и потому  $N^2 - D = 0$ .

$\sqrt{D} \pmod{M}$  (причем значения  $x, y$  мы все время предполагаем взаимно простыми), то из этого могут быть выведены несколько собственных преобразований формы  $F = (a, b, c)$  в форму  $G = (M, N, (N^2 - D)/M)$ . Именно, если представление получается при значениях  $x = m', y = n'$ , то  $F$  будет переводиться в  $G$  подстановкой

$$x = m'x' + \frac{m'N - m'b - n'c}{M}y', \quad y = n'x' + \frac{n'N + m'a + n'b}{M}y'.$$

Обратно, из каждого собственного преобразования формы  $F$  в  $G$  получается представление числа  $M$  формой  $F$ , принадлежащее значению  $N$ . Именно, если  $F$  переходит в  $G$  при подстановке  $x = mx' - \nu y', y = nx' + \mu y'$ , то  $M$  будет представляться формой  $F$ , если положить  $x = m, y = n$ , и так как здесь  $m\mu + n\nu = 1$ , значение выражения  $\sqrt{D} \pmod{M}$ , которому принадлежит представление, будет равно  $\mu(bt + cn) - \nu(at + bn)$ , т. е.  $N$ . Из нескольких различных собственных преобразований будет получаться столько же различных принадлежащих  $N$  представлений\*. Отсюда легко следует, что если имеются все собственные преобразования формы  $F$  в  $G$ , то из них можно получить все принадлежащие значению  $N$  представления числа  $M$  формой  $F$ . Таким образом, задача об отыскании представлений заданного числа заданной формой (при которых неизвестные имеют взаимно простые значения) сводится к задаче об отыскании всех собственных преобразований этой формы в заданную эквивалентную ей форму.

Если использовать здесь то, что было изложено в п. 162, то легко получается, что если одно из принадлежащих значению  $N$  представлений числа  $M$  формой  $F$  есть  $x = \alpha, y = \gamma$ , то общая формула, охватывающая все принадлежащие значению  $N$  представления того же числа формой  $F$ , такова:

---

\* Если мы предположим, что из двух преобразований получается одно и то же представление, то эти преобразования должны иметь вид

$$1) \ x = mx' - \nu y', \quad y = nx' + \mu y'; \quad 2) \ x = mx' - \nu' y', \quad y = nx' + \mu' y'.$$

Но из двух равенств

$m\mu + n\nu = m\mu' + n\nu', \quad \mu(mt + nc) - \nu(mt + nb) = \mu'(mt + nc) - \nu'(mt + nb)$  легко видеть, что либо  $M = 0$ , либо  $\mu = \mu', \nu = \nu'$ . Случай  $M = 0$  мы, однако, исключили.

$$x = \frac{\alpha t - (\alpha b + \gamma c) u}{m}, \quad y = \frac{\gamma t - (\alpha a + \gamma b) u}{m},$$

где  $m$  есть наибольший общий делитель чисел  $a, 2b, c$ , а  $t, u$  обозначают произвольные числа, удовлетворяющие уравнению  $t^2 - Du^2 = m^2$ .

## 170

Если форма  $(a, b, c)$  эквивалентна какой-нибудь двусторонней форме, а значит как собственно, так и несобственно эквивалентна форме  $G = (M, N, (N^2 - D)/M)$ , или собственно эквивалентна как форме  $(M, N, (N^2 - D)/M)$ , так и форме  $(M, -N, (N^2 - D)/M)$ , то получаются представления формой  $F$  числа  $M$ , которые принадлежат как значению  $N$ , так и значению  $-N$ . И обратно, если имеется несколько представлений числа  $M$  этой формой  $F$ , которые принадлежат противоположным значениям  $N$  и  $-N$  выражения  $\sqrt{D} \pmod{M}$ , то форма  $F$  эквивалентна форме  $G$  как собственно, так и несобственно, и может быть найдена двусторонняя форма, которой  $F$  эквивалентна.

Этими общими замечаниями о представлениях в этом месте можно ограничиться. О представлениях, в которых неизвестные имеют не взаимно простые значения, мы будем говорить ниже. В отношении остальных свойств формы с отрицательными определителями надо исследовать совсем другими способами, чем формы с положительными определителями. Поэтому мы будем теперь рассматривать формы с отрицательными и положительными определителями отдельно и начнем с первых как более легких.

## О формах с отрицательным определителем

## 171

**Задача.** Пусть дана какая-нибудь форма  $(a, b, a')$ , определитель которой отрицателен и равен  $-D$ , где  $D$  обозначает положительное число; найти собственно эквивалентную ей форму  $(A, B, C)$ , у которой  $A$  не больше чем  $\sqrt{4D/3}$  и  $C$ , и не меньше чем  $2B$ .

**Решение.** Мы предположим, что для заданной формы не выполняются одновременно все три условия, так как иначе не нужно было бы искать другую форму. Пусть  $b'$  — абсолютно наименьший вычет числа  $-b$  по модулю  $a' *$ , и  $a'' = \frac{b'^2 + D}{a'}$  (это число целое, так как  $b'^2 \equiv b^2$ ,  $b'^2 + D \equiv b^2 + D \equiv aa' \equiv 0 \pmod{a'}$ ). Если теперь  $a'' < a'$ , то пусть снова  $b''$  — абсолютно наименьший вычет числа  $-b'$  по модулю  $a''$ , и  $a''' = \frac{b''^2 + D}{a''}$ . Если и здесь еще  $a''' < a''$ , то пусть снова  $b'''$  — абсолютно наименьший вычет числа  $-b''$  по модулю  $a'''$ , и  $a'''' = \frac{b'''^2 + D}{a'''}$ . Эту операцию продолжаем до тех пор, пока в ряду  $a', a'', a''', a'''', \dots$  не достигнем члена  $a^{(m+1)}$ , который не меньше, чем предшествующий ему  $a^{(m)}$ ; это в конце концов должно случиться, потому что иначе получился бы бесконечный ряд все время убывающих целых чисел. Тогда форма  $(a^{(m)}, b^{(m)}, a^{(m+1)})$  будет удовлетворять всем условиям.

**Доказательство. I.** В ряду форм  $(a, b, a')$ ,  $(a', b', a'')$ ,  $(a'', b'', a''')$ , ... каждая является соседней для предыдущей, поэтому последняя собственно эквивалентна первой (пп. 159, 160).

**II.** Так как  $b^{(m)}$  есть абсолютно наименьший вычет числа  $-b^{(m-1)}$  по модулю  $a^{(m)}$ , то  $b^{(m)}$  не может быть больше чем  $a^{(m)}/2$  (п. 4).

**III.** Так как  $a^{(m)} a^{(m+1)} = D + b^{(m)2}$  и  $a^{(m+1)}$  не меньше чем  $a^{(m)}$ , то  $a^{(m)2}$  будет не больше, чем  $D + b^{(m)2}$ , и так как  $b^{(m)}$  не больше чем  $a^{(m)}/2$ , то  $a^{(m)2}$  будет не больше чем  $D + \frac{1}{4} a^{(m)2}$ , и потому  $3a^{(m)2}/4$  будет не больше чем  $D$  и, наконец,  $a^{(m)}$  — не больше чем  $\sqrt{4D/3}$ .

**Пример.** Пусть задана форма  $(304, 217, 155)$ , определитель которой равен  $-31$ . Здесь мы находим такой ряд форм:

$$(304, 217, 155), \quad (155, -62, 25), \quad (25, 12, 7), \\ (7, 2, 5), \quad (5, -2, 7).$$

---

\* Заметим, что если у формы  $(a, b, a')$  равен 0 первый член  $a$  или последний член  $a'$ , то определитель этой формы будет положительным квадратом; следовательно, в настоящем случае указанное обстоятельство не может иметь места. По аналогичной причине крайние члены  $a, a'$  формы с отрицательным определителем не могут иметь противоположных знаков.

Последняя является искомой. Точно так же для формы (121, 49, 20), определитель которой равен  $-19$ , находим эквивалентные формы (20,  $-9$ , 5), (5,  $-1$ , 4), (4, 1, 5); тем самым (4, 1, 5) есть искомая форма.

Такие формы  $(A, B, C)$ , определители которых отрицательны и у которых  $A$  не больше чем  $\sqrt{4D/3}$  и  $C$ , и не меньше чем  $2B$ , мы будем называть приведенными формами. Итак, для каждой формы с отрицательным определителем может быть найдена собственно эквивалентная ей приведенная форма.

## 172

**Задача.** Найти условия, при которых две различные приведенные формы  $(a, b, c)$  и  $(a', b', c')$  с одним и тем же определителем  $-D$  могут быть собственно эквивалентны.

**Решение.** Если мы предположим (что допустимо), что  $a'$  не больше чем  $a$ , и что форма  $ax^2 + 2bxy + cy^2$  переходит в форму  $a'x'^2 + 2b'x'y' + c'y'^2$  при собственной подстановке  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$ , то мы имеем равенства:

$$[1] \quad a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a',$$

$$[2] \quad a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b',$$

$$[3] \quad \alpha\delta - \beta\gamma = 1.$$

Из [1] следует, что  $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$ , поэтому произведение  $aa'$  положительно, а так как  $ac = D + b^2$ ,  $a'c' = D + b'^2$ , то  $ac$  и  $a'c'$  тоже положительно. Поэтому все числа  $a, a', c, c'$  имеют одинаковые знаки. Так как теперь как  $a$ , так и  $a'$  не больше чем  $\sqrt{4D/3}$ , то  $aa'$  не больше чем  $4D/3$ , и тем самым  $D\gamma^2$  (которое равно  $aa' - (a\alpha + b\gamma)^2$ ) подавно не может быть больше чем  $4D/3$ . Следовательно,  $\gamma$  или равно нулю, или равно  $\pm 1$ .

I. Если  $\gamma = 0$ , то из [3] следует, что или  $\alpha = 1, \delta = 1$ , или  $\alpha = -1, \delta = -1$ . В обоих случаях из [1] получается  $a' = a$ , а из [2] вытекает, что  $b' - b = \pm \beta a$ . Но  $b$  не больше чем  $a/2$ , и  $b'$  не больше чем  $a'/2$ , и потому также не больше чем  $a/2$ . Поэтому равенство  $b' - b = \pm \beta a$  может выполняться только тогда, когда:

или  $b = b'$ ; тогда отсюда следовало бы  $c' = \frac{b'^2 + D}{a'} = \frac{b^2 + D}{a} = c$ , т. е., вопреки предположению, формы  $(a, b, c)$  и  $(a', b', c')$  совпадали бы;

или  $b = -b' = \pm \frac{1}{2} a$ ; в этом случае  $c' = c$ , и форма  $(a', b', c')$  переходит в  $(a, -b, c)$ , т. е. в форму, противоположную форме  $(a, b, c)$ . Одновременно получается, что эти формы двусторонние, так как  $2b = \pm a$ .

II. Если  $\gamma = \pm 1$ , то из [1] получается  $a\alpha^2 + c - a' = \pm 2b\alpha$ . Так как, однако,  $c$  не меньше чем  $a$ , и потому не меньше чем  $a'$ , то  $a\alpha^2 + c - a'$  или  $2b\alpha$ , очевидно, не меньше чем  $a\alpha^2$ . Поэтому, так как  $2b$  не больше чем  $a$ ,  $\alpha$  будет не меньше чем  $\alpha^2$ ; а отсюда необходимо следует, что  $\alpha = 0$  или  $\alpha = \pm 1$ .

1. Если  $\alpha = 0$ , то из [1] будет вытекать  $a' = c$ , и так как  $a$  не больше чем  $c$  и не меньше чем  $a'$ , то обязательно будет  $a' = a = c$ . Далее, из [3] следует, что  $\beta\gamma = -1$ , и потому из [2] получается  $b + b' = \pm \delta c = \pm \delta a$ . Отсюда, подобно тому, как в I, вытекает, что или  $b = b'$ ; в этом случае формы  $(a, b, c)$ ,  $(a', b', c')$ , вопреки предположению, совпадали бы;

или  $b = -b'$ ; в этом случае формы  $(a, b, c)$ ,  $(a', b', c')$  противоположны.

2. Если  $\alpha = \pm 1$ , то из 1 следует, что  $\pm 2b = a + c - a'$ , и так как ни  $a$ , ни  $c$  не меньше чем  $a'$ , то  $2b$  будет не меньше чем  $a$  и не меньше чем  $c$ . Но  $2b$  также не больше чем  $a$  и не больше чем  $c$ ; поэтому обязательно  $\pm 2b = a = c$ , а вследствие равенства  $\pm 2b = a + c - a'$  равно также и  $a'$ . Таким образом, из [2] получается

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma),$$

или, вследствие того, что  $\alpha\delta - \beta\gamma = 1$ ,

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma);$$

поэтому, как и раньше, обязательно

или  $b = b'$ , откуда, вопреки предположению, получалось бы, что формы  $(a, b, c)$ ,  $(a', b', c')$  совпадают;

или  $b = -b'$ , когда эти формы противоположны. Вследствие того,

что  $a = \pm 2b$ , формы в этом случае одновременно будут двусторонними.

Из всего этого следует, что формы  $(a, b, c)$  и  $(a', b', c')$  только тогда могут быть собственно эквивалентными, когда они противоположны и одновременно или являются двусторонними, или имеет место  $a = c = a' = c'$ . То, что в этих случаях формы  $(a, b, c)$  и  $(a', b', c')$  собственно эквивалентны, также легко усматривается из предыдущего. Действительно, если формы противоположны, они должны быть эквивалентны несобственно, а если они, кроме того, двусторонние, то также и собственно. Если же  $a = c$ , то форма  $(\frac{D+(a-b)^2}{a}, a-b, a)$  будет соседней для формы  $(a, b, c)$ , и потому эквивалентна ей. Но вследствие того, что  $D + b^2 = ac = a^2$ , имеет место  $\frac{D+(a-b)^2}{a} = 2a - 2b$ , и форма  $(2a - 2b, a - b, a)$  — двусторонняя. Поэтому форма  $(a, b, c)$  будет также и собственно эквивалентна своей противоположной.

Так же легко можно теперь узнавать, когда две не противоположные приведенные формы  $(a, b, c)$  и  $(a', b', c')$  могут быть несобственно эквивалентными. Именно, они будут несобственно эквивалентны, если формы  $(a, b, c)$  и  $(a', -b', c')$ , которые не совпадают, собственно эквивалентны, и обратно. Отсюда вытекает, что условие, при котором первые формы несобственно эквивалентны, заключается в том, что они совпадают, и, кроме того, или они двусторонние, или  $a = c$ . Приведенные же формы, которые не совпадают и не противоположны, не могут быть эквивалентны ни собственно, ни несобственно.

**Задача.** Пусть даны две формы  $F$  и  $F'$  с одинаковым отрицательным определителем; требуется узнать, эквивалентны ли они.

**Решение.** Найдем обе приведенные формы  $f, f'$ , которые собственно эквивалентны соответственно формам  $F, F'$ . Если тогда формы  $f, f'$  эквивалентны собственно, или несобственно, или обоими способами, то так же эквивалентны будут и  $F, F'$ . Если же  $f, f'$  не эквивалентны никаким способом, то не будут никаким способом эквивалентны и  $F, F'$ .



Согласно предыдущему пункту, может представиться четыре случая.

1. Если  $f, f'$  не совпадают и не противоположны, то  $F, F'$  не эквивалентны никаким способом.

2. Если  $f, f'$ , во-первых, или совпадают, или противоположны, и, во-вторых, или являются двусторонними, или имеют какие-нибудь равные крайние члены, то  $F, F'$  будут эквивалентны как собственно, так и несобственно.

3. Если  $f, f'$  совпадают, но не являются двусторонними и не имеют равных крайних членов, то  $F, F'$  будут только собственно эквивалентны.

4. Если  $f, f'$  противоположны, но не являются двусторонними и не имеют равных крайних членов, то  $F, F'$  будут только несобственно эквивалентны.

**Пример.** Для форм (41, 35, 30), (7, 18, 47), определители которых равны — 5, приведенные формы (1, 0, 5), (2, 1, 3) оказываются не эквивалентными. Поэтому первые формы не эквивалентны никаким способом. Формам же (23, 38, 63), (15, 20, 27) эквивалентна одна и та же приведенная форма (2, 1, 3), и, так как она одновременно является двусторонней, то формы (23, 38, 63), (15, 20, 27) будут эквивалентны как собственно, так и несобственно. Формам (37, 53, 78) и (53, 73, 102) эквивалентны приведенные формы (9, 2, 9), (9, — 2, 9), и так как они противоположны и их крайние члены равны, то заданные формы будут эквивалентны как собственно, так и несобственно.

#### 174

*Число всех приведенных форм, которые имеют данный определитель —  $D$ , всегда конечно и не очень велико в сравнении с числом  $D$ . Сами же эти формы могут быть найдены двумя способами. Мы будем обозначать произвольные приведенные формы с определителем —  $D$  через  $(a, b, c)$ ; таким образом, должны быть определены все значения  $a, b, c$ .*

**Первый метод.** За  $a$  берутся все числа, как положительные, так и отрицательные, которые не больше чем  $\sqrt{4D/3}$  и по которым —  $D$  есть квадратичный вычет, и для отдельных  $a$  число  $b$

последовательно полагается равным всем, как положительным, так и отрицательным значениям выражения  $\sqrt{-D} \pmod{a}$ , которые не больше, чем  $a/2$ ; с для отдельных определенных значений  $a$ ,  $b$  полагается равным  $(D - b^2)/a$ . Если при этом получатся какие-нибудь формы, у которых  $s < a$ , то их нужно выбросить; остальные же, очевидно, будут приведенными.

**Второй метод.** За  $b$  берутся все числа, как положительные, так и отрицательные, которые не больше чем  $\frac{1}{2}\sqrt{\frac{4}{3}D}$  или  $\sqrt{D/3}$ , для отдельных  $b$  выражение  $b^2 + D$  раскладывается всеми возможными способами (учитывая и различие знаков) на такие два сомножителя, которые оба не меньше чем  $2b$ , и один из сомножителей, причем, если они не равны, то меньший полагается равным  $a$ , а другой равным  $s$ . Так как  $a$  не больше чем  $\sqrt{4D/3}$ , то все получающиеся при этом формы, очевидно, будут приведенными. Наконец, ясно, что не может быть никакой приведенной формы, которая не была бы найдена каждым из двух методов.

**Пример.** Пусть  $D = 85$ . Здесь граница значений  $a$  равна числу  $\sqrt{340/3}$ , которое лежит между 10 и 11. Числа же между 1 и 10 (включительно), по которым  $-85$  есть вычет, суть 1, 2, 5, 10. Отсюда получается двенадцать форм:

$$(1, 0, 85), (2, 1, 43), (2, -1, 43), (5, 0, 17), (10, 5, 11), \\ (10, -5, 11), (-1, 0, -85), (-2, 1, -43), (-2, -1, -43), \\ (-5, 0, -17), (-10, 5, -11), (-10, -5, -11).$$

При другом методе в качестве границы для значений  $b$  получаетя число  $\sqrt{85/3}$ , которое лежит между 5 и 6. Для  $b = 0$  получаются формы  $(1, 0, 85)$ ,  $(-1, 0, -85)$ ,  $(5, 0, 17)$ ,  $(-5, 0, -17)$ ; для  $b = \pm 1$  — формы  $(2, \pm 1, 43)$ ,  $(-2, \pm 1, -43)$ . Для  $b = \pm 2$  не получается ничего, так как 89 не может быть разложено на два сомножителя, которые оба не меньше чем 4. То же имеет место для  $\pm 3$ ,  $\pm 4$ . Наконец, из  $b = \pm 5$  получаются следующие формы:  $(10, \pm 5, 11)$ ,  $(-10, \pm 5, -11)$ .

Если среди всех приведенных форм с данным определителем из каждых двух форм, которые не совпадают, но собственно эквива-

лентны, выбросить ту или иную, то оставшиеся формы обладают тем замечательным свойством, что любая форма с тем же определителем собственно эквивалентна какой-нибудь из них, причем только одной (так как иначе среди них были бы собственно эквивалентные). Отсюда вытекает, что *все формы с тем же самым определителем могут быть разбиты на столько классов, сколько осталось форм*, именно, если причислять к одному классу формы, собственно эквивалентные одной и той же приведенной форме. Так, например, для  $D = 85$  остаются формы

$$(1, 0, 85), (2, 1, 43), (5, 0, 17), (10, 5, 11),$$

$$(-1, 0, -85), (-2, 1, -43), (-5, 0, -17), (-10, 5, -11),$$

так что все формы с определителем  $-85$  могут быть разбиты на восемь классов, в зависимости от того, эквивалентны ли они первой, второй и т. д. форме. Очевидно, что формы, помещенные в один класс, собственно эквивалентны, а формы из различных классов, напротив, не могут быть собственно эквивалентными. Впрочем, этот вопрос о классификации форм мы значительно подробнее будем рассматривать ниже. Здесь мы добавим только единственное замечание. Выше мы уже показали, что если определитель формы  $(a, b, c)$  отрицателен и равен  $-D$ , то  $a$  и  $c$  имеют одинаковые знаки (именно, потому что  $ac = b^2 + D$  и, значит, положительно). Из этих же соображений легко убедиться, что если формы  $(a, b, c)$ ,  $(a', b', c')$  эквивалентны, то все величины  $a, c, a', c'$  будут иметь одинаковые знаки. Действительно, если первая переходит во вторую при подстановке  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$ , то  $a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$ , и отсюда  $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$ , и потому, очевидно, неотрицательно. Так как, однако, ни  $a$ , ни  $a'$  не могут быть равны нулю, то  $aa'$  будет положительно и, следовательно, знаки у  $a, a'$  будут одинаковы.

Поэтому ясно, что формы, крайние члены которых положительны, совершенно обособливаются от тех, крайние члены которых отрицательны, и можно рассматривать только те из приведенных форм, которые имеют положительные крайние члены, так как остальные имеются в таком же количестве и получаются из первых, если крайним членам придаются противоположные знаки; и точно так же обстоит дело для форм, которые выбрасываются или оставляются среди приведенных.

Здесь для некоторых отрицательных определителей дана таблица форм, по которым все остальные формы с тем же определителем могут быть разделены на классы. В соответствии с замечаниями в предыдущем пункте мы помещаем, однако, только половину форм, именно, те, крайние члены которых положительны.

| $D$ | Формы                                        |
|-----|----------------------------------------------|
| 1   | (1, 0, 1)                                    |
| 2   | (1, 0, 2)                                    |
| 3   | (1, 0, 3), (2, 1, 2)                         |
| 4   | (1, 0, 4), (2, 0, 2)                         |
| 5   | (1, 0, 5), (2, 1, 3)                         |
| 6   | (1, 0, 6), (2, 0, 3)                         |
| 7   | (1, 0, 7), (2, 1, 4)                         |
| 8   | (1, 0, 8), (2, 0, 4), (3, 1, 3)              |
| 9   | (1, 0, 9), (2, 1, 5), (3, 0, 3)              |
| 10  | (1, 0, 10), (2, 0, 5)                        |
| 11  | (1, 0, 11), (2, 1, 6), (3, 1, 4), (3, -1, 4) |
| 12  | (1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4)  |

Продолжать здесь эту таблицу дальше было бы излишне, так как ниже мы покажем значительно более целесообразное ее устройство.

Итак, очевидно, что каждая форма с определителем  $-1$  собственно эквивалентна форме  $x^2 + y^2$ , если ее крайние члены положительны, и форме  $-x^2 - y^2$ , если они отрицательны. Далее, каждая форма с определителем  $-2$ , крайние члены которой положительны, будет собственно эквивалентна форме  $x^2 + 2y^2$ , так же как каждая форма с определителем  $-11$ , крайние члены которой положительны, собственно эквивалентна одной из форм  $x^2 + 11y^2$ ,  $2x^2 + 2xy + 6y^2$ ,  $3x^2 + 2xy + 4y^2$ ,  $3x^2 - 2xy + 4y^2$ .

## 177

**Задача.** Имеется ряд форм, каждая из которых является соседней справа для предыдущей; требуется найти какое-нибудь собственное преобразование первой формы в любую форму ряда.

**Решение.** Пусть заданные формы суть

$$(a, b, a') = F, \quad (a', b', a'') = F', \quad (a'', b'', a''') = F'', \quad (a''', b''', a''') = F''', \dots$$

Величины  $(b + b')/a'$ ,  $(b' + b'')/a''$ ,  $(b'' + b''')/a'''$ , ... обозначим соответственно через  $h'$ ,  $h''$ ,  $h'''$ , ..., а неизвестные формы  $F$ ,  $F'$ ,  $F''$ , ... пусть соответственно  $x, y$ ;  $x', y'$ ;  $x'', y''$ ; ... Далее, предположим, что  $F$  должна переходить

$$\begin{array}{ll} \text{в } F' \text{ , если положить } x = \alpha'x' + \beta'y', & y = \gamma'x' + \delta'y', \\ \text{в } F'' \text{ , } \gg \gg x = \alpha''x'' + \beta''y'', & y = \gamma''x'' + \delta''y'', \\ \text{в } F''' \text{ , } \gg \gg x = \alpha'''x''' + \beta'''y''', & y = \gamma'''x''' + \delta'''y''', \end{array}$$

и т. д.

Тогда, так как

$$\begin{array}{llll} F \text{ переходит в } F' \text{ , если положить } x = -y', & y = x' + h'y' \\ F' \gg \gg F'' \gg \gg x' = -y'', & y' = x'' + h''y'', \\ F'' \gg \gg F''' \gg \gg x'' = -y''', & y'' = x''' + h'''y''', \end{array}$$

и т. д. (п. 160),

легко выводится следующий алгоритм (п. 159):

$$\begin{array}{llll} \alpha' = 0, & \beta' = -1, & \gamma' = 1, & \delta' = h', \\ \alpha'' = \beta', & \beta'' = h''\beta' - \alpha', & \gamma'' = \delta', & \delta'' = h''\delta' - \gamma', \\ \alpha''' = \beta'', & \beta''' = h''' \beta'' - \alpha'', & \gamma''' = \delta'', & \delta''' = h''' \delta'' - \gamma'', \\ \alpha'''' = \beta''', & \beta'''' = h'''' \beta''' - \alpha''', & \gamma'''' = \delta''', & \delta'''' = h'''' \delta''' - \gamma''', \end{array}$$

и т. д.,

или

$$\begin{array}{llll} \alpha' = 0, & \beta' = -1, & \gamma' = 1, & \delta' = h', \\ \alpha'' = \beta', & \beta'' = h''\beta', & \gamma'' = \delta', & \delta'' = h''\delta' - 1, \\ \alpha''' = \beta'', & \beta''' = h''' \beta'' - \beta', & \gamma''' = \delta'', & \delta''' = h''' \delta'' - \delta', \\ \alpha'''' = \beta''', & \beta'''' = h'''' \beta''' - \beta'', & \gamma'''' = \delta''', & \delta'''' = h'''' \delta''' - \delta'', \end{array}$$

и т. д.

То, что все эти преобразования собственные, без труда может быть выведено как из их образования, так и из п. 159.

Этот очень простой и удобный при вычислениях алгоритм аналогичен алгоритму, изложенному в п. 27, и может быть сведен к нему\*. Впрочем, это решение не ограничивается формами с отрицательными определителями, а распространяется на все случаи, если только ни одно из чисел  $a'$ ,  $a''$ ,  $a'''$ , ... не равно нулю.

## 178

**Задача.** Даны две собственно эквивалентные формы  $F$ ,  $f$  с одним и тем же отрицательным определителем; найти какое-нибудь собственное преобразование одной формы в другую.

**Решение.** Предположим, что форма  $F$  есть  $(A, B, A')$ , и что методом п. 171 найден ряд форм  $(A', B', A'')$ ,  $(A'', B'', A''')$ , ...,  $(A^{(m)}, B^{(m)}, A^{(m+1)})$ , последняя из которых приведенная; точно так же, предположим, что форма  $f$  есть  $(a, b, a')$ , и что тем же методом найден ряд форм  $(a', b', a'')$ ,  $(a'', b'', a''')$ , ...,  $(a^{(n)}, b^{(n)}, a^{(n+1)})$ , последняя из которых приведенная. Тогда могут представиться два случая.

I. Формы  $(A^{(m)}, B^{(m)}, A^{(m+1)})$ ,  $(a^{(n)}, b^{(n)}, a^{(n+1)})$  или совпадают, или противоположны и одновременно двусторонние. Тогда формы  $(A^{(m-1)}, B^{(m-1)}, A^{(m)})$  и  $(a^{(n)}, -b^{(n-1)}, a^{(n-1)})$  будут соседними (здесь  $A^{(m-1)}$  обозначает предпоследний член ряда  $A, A', A'', \dots, A^{(m)}$ , и  $B^{(m-1)}, a^{(n-1)}, b^{(n-1)}$  имеют подобное же значение). Действительно,  $A^{(m)} = a^{(n)}$ ,  $B^{(m-1)} \equiv -B^{(m)} \pmod{A^{(m)}}$ ,  $b^{(n-1)} \equiv -b^{(n)} \pmod{a^{(n)} \text{ или } A^{(m)}}$ ,

\* Именно, в обозначениях п. 27,

$$\beta^{(n)} = \pm [-h'', h''', -h''', \dots, \pm h^{(n)}],$$

где двойные знаки должны иметь значения  $---$ ,  $-+$ ,  $+-$ ,  $++$ , если  $n$  имеет соответственно вид  $4k + 0, 1, 2, 3$ , и

$$\delta^{(n)} = \pm [h', -h'', h''', \dots, \pm h^{(n)}],$$

где двойные знаки имеют значения  $+-$ ,  $++$ ,  $---$ ,  $-+$ , когда  $n$  соответственно имеет вид  $4k + 0, 1, 2, 3$ . Ради краткости, мы, однако, не будем вдаваться в это подробнее; впрочем, убедиться в этом каждый легко может и сам.

поэтому  $B^{(m-1)} - b^{(n-1)} \equiv b^{(n)} - B^{(m)}$ , и потому  $\equiv 0$ , если формы  $(A^{(m)}, B^{(m)}, A^{(m+1)})$ ,  $(a^{(n)}, b^{(n)}, a^{(n+1)})$  совпадают, и  $\equiv 2b^{(n)}$  и тем самым  $\equiv 0$ , если они противоположны и одновременно двусторонние. Поэтому в ряду форм

$$(A, B, A'), (A', B', A''), \dots, (A^{(m-1)}, B^{(m-1)}, A^{(m)}),$$

$$(a^{(n)}, -b^{(n-1)}, a^{(n-1)}), (a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}), \dots, (a', -b, a), (a, b, a')$$

каждая форма — соседняя для предыдущей, и тем самым, согласно предыдущему пункту, может быть найдено собственное преобразование первой формы  $F$  в последнюю форму  $f$ .

II. Формы  $(A^{(m)}, B^{(m)}, A^{(m+1)})$ ,  $(a^{(n)}, b^{(n)}, a^{(n+1)})$  не совпадают, но противоположны и одновременно  $A^{(m)} = A^{(m+1)} = a^{(n)} = a^{(n+1)}$ . Тогда ряд форм

$$(A, B, A'), (A', B', A''), \dots, (A^{(m)}, B^{(m)}, A^{(m+1)}),$$

$$(a^{(n)}, -b^{(n-1)}, a^{(n-1)}), (a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}), \dots, (a', -b, a), (a, b, a')$$

будет обладать тем же свойством. Действительно,  $A^{(m+1)} = a^{(n)}$  и  $B^{(m)} - b^{(n-1)} = -(b^{(n)} + b^{(n-1)})$  делится на  $a^{(n)}$ . Тем самым, согласно предыдущему пункту, может быть найдено собственное преобразование первой формы  $F$  в последнюю форму  $f$ .

**Пример.** Так, для форм (23, 38, 63), (15, 20, 27) имеем ряд (23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, -7, 27), (27, -20, 15), (15, 20, 27). Поэтому

$$h' = 1, \quad h'' = 3, \quad h''' = 2, \quad h'''' = -3, \quad h''''' = -1, \quad h'''''' = 0.$$

Отсюда в качестве преобразования формы  $23x^2 + 76xy + 63y^2$  в форму  $15t^2 + 40tu + 27u^2$  получается следующее:  $x = -13t - 18u$ ,  $y = 8t + 11u$ .

Из этого решения без труда вытекает решение следующей задачи: пусть формы  $F$ ,  $f$  несобственно эквивалентны; найти несобственное преобразование формы  $F$  в  $f$ . Действительно, если  $f = at^2 + 2btu + a'u^2$ , то противоположная форма  $ap^2 - 2bpq + a'q^2$  собственно эквивалентна форме  $F$ . Если найдено собственное преобразование формы  $F$  в форму  $ap^2 - 2bpq + a'q^2$ , именно,  $x = \alpha p + \beta q$ ,  $y = \gamma p + \delta q$ , то  $F$ , очевидно, будет переходить в  $f$ , если положить  $x = \alpha t - \beta u$ ,  $y = \gamma t - \delta u$ , и это преобразование будет несобственным.

Если формы  $F, f$  эквивалентны как собственно, так и несобственно, то можно, таким образом, всегда найти как собственное, так и несобственное преобразование.

179

**Задача.** Пусть формы  $F, f$  эквивалентны; найти все преобразования  $F$  в  $f$ .

**Решение.** Если формы  $F, f$  эквивалентны только одним способом, т. е. только собственно или только несобственно, то найдем в соответствии с предыдущим пунктом одно преобразование формы  $F$  в  $f$ ; тогда ясно, что других преобразований, кроме тех, которые с ним однотипны, быть не может. Если же формы  $F, f$  эквивалентны как собственно, так и несобственно, то найдем два преобразования, одно собственное и одно несобственное. Если теперь  $F = (A, B, C)$ , далее,  $B^2 - AC = -D$ , и наибольший общий делитель чисел  $A, 2B, C$  равен  $m$ , то из п. 162 следует, что в первом случае все преобразования формы  $F$  в  $f$  могут быть выведены из одного преобразования, а во втором случае все собственные преобразования — из одного собственного, и все несобственные — из одного несобственного, если только имеются все решения уравнения  $t^2 + Du^2 = m^2$ . Итак, если они найдены, то задача решена.

Но мы имеем  $D = AC - B^2$ ,  $4D = 4AC - 4B^2$ , и потому число  $\frac{4D}{m^2} = 4\frac{AC}{m^2} - \left(\frac{2B}{m}\right)^2$  целое.

1. Если теперь  $\frac{4D}{m^2} > 4$ , то  $D > m^2$ , поэтому в  $t^2 + Du^2 = m^2$  обязательно должно быть  $u = 0$ , и тем самым  $t$  не может иметь других значений, кроме  $+m$  или  $-m$ . Если поэтому  $F, f$  эквивалентны только одним способом и какое-нибудь преобразование есть

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

то, кроме этого преобразования, которое получается из  $t = m$  (п. 162), и следующего:

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y',$$



других преобразований быть не может. Если же  $F, f$  эквивалентны как собственным, так и несобственным, и имеется какое-нибудь собственное преобразование

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

и несобственное преобразование

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y',$$

то собственных преобразований, кроме первого (получающегося из  $t = m$ ) и следующего (получающегося из  $t = -m$ ):

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y',$$

не будет, и аналогичным образом не будет несобственных преобразований, кроме

$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$  и  $x = -\alpha' x' - \beta' y', \quad y = -\gamma' x' - \delta' y'$ .

2. Если  $\frac{4D}{m^2} = 4$  или  $D = m^2$ , то уравнение  $t^2 + Du^2 = m^2$  допускает четыре решения, именно:  $t, u = m, 0; -m, 0; 0, 1; 0, -1$ . Если поэтому  $F, f$  эквивалентны только одним способом, и одно из преобразований есть

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

то всего имеется четыре преобразования:

$$x = \pm \alpha x' \pm \beta y', \quad y = \pm \gamma x' \pm \delta y',$$

$$x = \mp \frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y', \quad y = \pm \frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'.$$

Если же  $F, f$  эквивалентны двумя способами или, кроме указанного данного преобразования, имеется еще одно, неоднотипное с ним, то оно принесет тоже четыре преобразования, неоднотипных с первым, так что имеется восемь преобразований. Впрочем, легко доказать, что в этом случае  $F, f$  всегда действительно эквивалентны двумя способами. Действительно, так как  $D = m^2 = AC - B^2$ , то  $m$  входит также и в  $B$ . Определитель формы  $(A/m, B/m, C/m)$  равен  $-1$ , поэтому форма эквивалентна или форме  $(1, 0, 1)$ , или форме  $(-1, 0, -1)$ . Но легко видеть, что тем же преобразованием.

которым форма  $(A/m, B/m, C/m)$  переводится в  $(\pm 1, 0, \pm 1)$ , также и  $(A, B, C)$  переводится в форму  $(\pm m, 0, \pm m)$ , которая является двусторонней. Поэтому форма  $(A, B, C)$ , так как она эквивалентна двусторонней форме, будет эквивалентна как собственно, так и несобственно каждой форме, которой она эквивалентна вообще.

3. Если  $\frac{4D}{m^2} = 3$  или  $4D = 3m^2$ , то  $m$  четно, и всевозможными решениями уравнения  $t^2 + Du^2 = m^2$  являются следующие шесть:  
 $t, u = m, 0; -m, 0; \frac{1}{2}m, 1; -\frac{1}{2}m, 1; \frac{1}{2}m, -1; -\frac{1}{2}m, -1$ .

Если поэтому имеется два неотнотипных преобразования формы  $F$  в  $f$ :

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y',$$

то имеется двенадцать преобразований, именно, шесть, однотипных с первым:

$$x = \pm \alpha x' \pm \beta y', \quad y = \pm \gamma x' \pm \delta y',$$

$$\begin{cases} x = \pm \left( \frac{1}{2} \alpha - \frac{\alpha B + \gamma C}{m} \right) x' \pm \left( \frac{1}{2} \beta - \frac{\beta B + \delta C}{m} \right) y', \\ y = \pm \left( \frac{1}{2} \gamma + \frac{\alpha A + \gamma B}{m} \right) x' \pm \left( \frac{1}{2} \delta + \frac{\beta A + \delta B}{m} \right) y'; \end{cases}$$

$$\begin{cases} x = \pm \left( \frac{1}{2} \alpha + \frac{\alpha B + \gamma C}{m} \right) x' \pm \left( \frac{1}{2} \beta + \frac{\beta B + \delta C}{m} \right) y', \\ y = \pm \left( \frac{1}{2} \gamma - \frac{\alpha A + \gamma B}{m} \right) x' \pm \left( \frac{1}{2} \delta - \frac{\beta A + \delta B}{m} \right) y'; \end{cases}$$

и шесть однотипных со вторым, которые получаются из предыдущих, если вместо  $\alpha, \beta, \gamma, \delta$  подставить соответственно  $\alpha', \beta', \gamma', \delta'$ .

То, что в этом случае  $F, f$  всегда эквивалентны обоими способами, доказывается следующим образом. Определитель формы  $(2A/m, 2B/m, 2C/m)$  равен  $-\frac{4D}{m^2} = -3$ , и потому (п. 176) эта форма эквивалентна или форме  $(\pm 1, 0, \pm 3)$ , или форме  $(\pm 2, \pm 1, \pm 2)$ . Из этого легко видно, что форма  $(A, B, C)$  эквивалентна или форме  $(\pm \frac{1}{2}m, 0, \pm \frac{3}{2}m)$ , или форме  $(\pm m, \frac{1}{2}m, \pm m)^*$ , которые обе дву-

\* Можно показать, что  $(A, B, C)$  обязательно эквивалентна второй из этих форм; однако это не является здесь необходимым.

сторонние, и потому каждая форма, эквивалентная форме  $(A, B, C)$  вообще, эквивалентна ей обоими способами.

4. Если предположить, что  $\frac{4D}{m^2} = 2$ , то  $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 2$ , и потому  $\equiv 2 \pmod{4}$ . Так как, однако, никакой квадрат не может быть  $\equiv 2 \pmod{4}$ , этот случай не может иметь места.

5. Если предположить, что  $\frac{4D}{m^2} = 1$ , то  $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 1 \equiv -1 \pmod{4}$ . Так как, однако, это невозможно, то и этот случай не может иметь места.

Так как, далее,  $D$  не равно нулю и неотрицательно, других случаев, кроме перечисленных, быть не может.

## 180

**Задача.** Требуется найти все представления заданного числа  $M$  формой  $F = ax^2 + 2bxy + cy^2$  с отрицательным определителем  $-D$ , у которых  $x, y$  имеют взаимно простые значения.

**Решение.** Из п. 154 явствует, что  $M$  может быть представлено желаемым способом только в том случае, если  $-D$  есть квадратичный вычет числа  $M$ . Поэтому сначала отыскиваются все различные, т. е. несравнимые значения выражения  $\sqrt{-D} \pmod{M}$ ; пусть эти значения суть  $N, -N, N', -N', N'', -N'', \dots$ . Для того чтобы вычисления были по возможности проще, все  $N, N', \dots$  могут быть определены так, чтобы они были не больше чем  $M/2$ . Так как каждое представление должно теперь принадлежать какому-нибудь одному из этих значений, можно рассматривать эти значения по отдельности.

Если формы  $F$  и  $(M, N, (D + N^2)/M)$  не являются собственно эквивалентными, то не может быть представления числа  $M$ , которое принадлежит значению  $N$  (п. 168). Если же они, напротив, собственно эквивалентны, то найдем собственное преобразование формы  $F$  в форму

$$Mx'^2 + 2Nx'y' + \frac{D + N^2}{M} y'^2.$$

Пусть это преобразование есть

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y';$$

тогда  $x = \alpha$ ,  $y = \gamma$  есть представление числа  $M$  формой  $F$ , принадлежащее  $N$ . Пусть наибольший общий делитель чисел  $A$ ,  $2B$ ,  $C$  равен  $m$ ; будем различать три случая (ср. предыдущий пункт).

1. Если  $\frac{4D}{m^2} > 4$ , то не может быть других принадлежащих  $N$  представлений, кроме следующих двух:  $x = \alpha$ ,  $y = \gamma$ ;  $x = -\alpha$ ,  $y = -\gamma$  (пп. 169, 179).

2. Если  $\frac{4D}{m^2} = 4$ , то имеется четыре представления:

$$x = \pm \alpha, \quad y = \pm \gamma; \quad x = \mp \frac{\alpha B + \gamma C}{m}, \quad y = \pm \frac{\alpha A + \gamma B}{m}.$$

3. Если  $\frac{4D}{m^2} = 3$ , то имеется шесть представлений:

$$x = \pm \alpha, \quad y = \pm \gamma;$$

$$x = \pm \left( \frac{1}{2} \alpha - \frac{\alpha B + \gamma C}{m} \right), \quad y = \pm \left( \frac{1}{2} \gamma + \frac{\alpha A + \gamma B}{m} \right);$$

$$x = \pm \left( \frac{1}{2} \alpha + \frac{\alpha B + \gamma C}{m} \right), \quad y = \pm \left( \frac{1}{2} \gamma - \frac{\alpha A + \gamma B}{m} \right).$$

Подобным же образом отыскиваются представления, принадлежащие значениям  $-N$ ,  $N'$ ,  $-N'$ ,...

Получение представлений числа  $M$  формой  $F$ , у которых  $x$ ,  $y$  имеют не взаимно простые значения, легко может быть сведено к уже рассмотренному случаю. Такое представление можно получить если положить  $x = \mu e$ ,  $y = \mu f$ , где  $\mu$  есть наибольший общий делитель  $\mu e$  и  $\mu f$ , т. е.  $e$  и  $f$  взаимно просты. Подстановка же  $x = e$ ,  $y = f$  будет представлением числа  $M / \mu^2$  формой  $F$ , в котором  $x$ ,  $y$  имеют взаимно простые значения. Если поэтому  $M$  не делится ни на какой квадрат (кроме 1), например, если оно есть простое число, то таких представлений числа  $M$  нет. Если же  $M$  содержит квадратные делители, то пусть они суть  $\mu^2$ ,  $\nu^2$ ,  $\pi^2$ ,... Сначала отыскиваются все представления формой  $(A, B, C)$  числа  $M / \mu^2$ , у которых  $x$ ,  $y$  имеют взаимно простые значения; эти значения, умноженные на  $\mu$ , дадут

все представления  $M$ ; у которых наибольший общий делитель  $x, y$  равен  $\mu$ . Подобным же образом все представления числа  $M/\nu^2$ , у которых значения  $x, y$  взаимно просты, дают все представления  $M$ , у которых наибольший общий делитель  $x, y$  равен  $\nu$ , и т. д.

Поэтому ясно, что при помощи предыдущих правил могут быть найдены все представления заданного числа заданной формой с отрицательным определителем.

### Специальные приложения к разложению чисел на два квадрата, на простой и удвоенный и на простой и утроенный квадраты

#### 182

Мы переходим к некоторым специальным случаям, отчасти вследствие их исключительного изящества, отчасти же потому, что ими подробно занимался Эйлер, благодаря чему они приобрели до некоторой степени классический характер.

I. Ни одно число, по которому  $-1$  не является квадратичным вычетом, не может быть представлено формой  $x^2 + y^2$  так, что  $x$  взаимно просто с  $y$  (или быть разложено на два взаимно простых квадрата); для всех остальных чисел, взятых положительными, это, напротив, возможно. Пусть  $M$  — такое число и пусть  $N, -N, N', -N', N'', -N'', \dots$  — всевозможные значения выражения  $\sqrt{-1} \pmod{M}$ . Тогда, согласно п. 176, форма  $(M, N, (N^2 + 1)/M)$  собственно эквивалентна форме  $(1, 0, 1)$ . Если  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$  — какое-нибудь собственное преобразование второй формы в первую, то принадлежащими  $N$  представлениями числа  $M$  формой  $x^2 + y^2$  являются следующие четыре:  $x = \pm \alpha$ ,  $y = \pm \gamma$ ;  $x = \mp \gamma$ ,  $y = \pm \alpha$  \*.

Так как форма  $(1, 0, 1)$  двусторонняя, то, очевидно, и форма  $(M, -N, (N^2 + 1)/M)$  будет ей собственно эквивалентна, и первая будет собственно преобразовываться во вторую, если положить  $x = \alpha x' - \beta y'$ ,  $y = -\gamma x' + \delta y'$ . Отсюда получаются четыре представления  $M$ , принадлежащих  $-N$ , именно:  $x = \pm \alpha$ ,  $y = \mp \gamma$ ;  $x = \pm \gamma$ ,  $y = \mp \alpha$ . Тем самым ясно, что имеется восемь представле-

\* Именно, этот случай содержится, очевидно, в п. 180, 2.

ний числа  $M$ , из которых половина принадлежит  $N$ , а половина принадлежит  $-N$ ; однако все они дают только одно единственное разложение числа  $M$  на два квадрата:  $M = \alpha^2 + \gamma^2$ , — если принимать во внимание только сами квадраты, а не порядок их расположения и не знаки корней из них.

Если поэтому других значений выражения  $\sqrt{-1} \pmod{M}$ , кроме  $N$  и  $-N$ , нет, что, например, имеет место, если число  $M$  простое, то  $M$  может быть только одним единственным способом разложено на два взаимно простых квадрата. А так как  $-1$  есть квадратичный вычет каждого простого числа вида  $4n + 1$  (п. 108), и простое число, очевидно, не может быть разложено на два не взаимно простых квадрата, то мы получаем следующую теорему.

*Каждое простое число вида  $4n + 1$  может быть разложено на два квадрата, причем одним единственным образом.*

Так, например,  $1 = 0 + 1$ ,  $5 = 1 + 4$ ,  $13 = 4 + 9$ ,  $17 = 1 + 16$ ,  $29 = 4 + 25$ ,  $37 = 1 + 36$ ,  $41 = 16 + 25$ ,  $53 = 4 + 49$ ,  $61 = 25 + 36$ ,  $73 = 9 + 64$ ,  $89 = 25 + 64$ ,  $97 = 16 + 81$ , ...

Эта в высшей степени изящная теорема была известна уже Ф е р м а, хотя впервые доказана была Э й л е р о м: «*Comm. nov, Petr.*», *T. V, 1754, 1755, S. 3* и сл. В четвертом томе, стр. 3 и далее, находится сочинение, посвященное этому же предмету, хотя тогда он еще и не закончил полностью эту работу (ср. особенно п. 27).

Поэтому, если какое-нибудь число вида  $4n + 1$  или может быть разложено на два квадрата несколькими способами, или не может быть разложено вообще, оно, очевидно, не является простым.

Наоборот, если выражение  $\sqrt{-1} \pmod{M}$ , кроме  $N$  и  $-N$ , имеет еще и другие значения, то будут и другие, принадлежащие этим значениям, представления числа  $M$ . В этом случае  $M$  может быть, таким образом, разложено на два квадрата несколькими способами, например,  $65 = 1 + 64 = 16 + 49$ ,  $221 = 25 + 196 = 100 + 121$ .

Остальные представления, в которых  $x$ ,  $y$  имеют не взаимно простые значения, легко могут быть найдены нашим общим методом. Заметим только, что если некоторое число, которое содержит сомножители вида  $4n + 3$ , не может быть освобождено от них делением на некоторый квадрат (что имеет место, если один или несколько из

этих сомножителей входят в нечетной степени), то оно никаким способом не может быть разложено на два квадрата\*.

II. Формой  $x^2 + 2y^2$  не может быть представлено так, что  $x$  взаимно просто с  $y$ , ни одно число, по которому  $-2$  является невычетом, в то время как для всех остальных чисел это возможно. Если  $-2$  есть вычет числа  $M$ , и  $N$  — какое-нибудь значение выражения  $\sqrt{-2} \pmod{M}$ , то (см. п. 176) формы  $(1, 0, 2)$  и  $(M, N, (N^2 + 2)/M)$  будут собственно эквивалентны. Если первая собственно переходит во вторую при подстановке  $x = \alpha x' + \beta y'$ ,  $y = \gamma x' + \delta y'$ , то  $x = \alpha$ ,  $y = \gamma$  будет принадлежащим  $N$  представлением числа  $M$ . Кроме него и представления  $x = -\alpha$ ,  $y = -\gamma$ , никакие другие значения  $N$  не принадлежат (п. 180).

Аналогично тому, как выше, убеждаемся, что представления  $x = \pm \alpha$ ,  $y = \mp \gamma$  принадлежат значению  $-N$ . Все эти четыре представления дают, однако, только одно разложение числа  $M$  на квадрат и удвоенный квадрат, и если кроме  $N$  и  $-N$  других значений выражения  $\sqrt{-2} \pmod{M}$  больше нет, то нет также и других представлений числа  $M$ . Отсюда при помощи теоремы п. 116 легко выводится следующая теорема.

*Каждое простое число вида  $8n + 1$  или  $8n + 3$  может быть разложено на квадрат и удвоенный квадрат и притом только одним способом.*

Так, например,  $1 = 1 + 0$ ,  $3 = 1 + 2$ ,  $11 = 9 + 2$ ,  $17 = 9 + 8$ ,

---

\* Если  $M = 2^\mu S \alpha^\alpha \beta^\beta \gamma^\gamma \dots$ , где  $\alpha, \beta, \gamma, \dots$  обозначают различные простые числа вида  $4n + 1$ , и  $S$  — произведение всех простых сомножителей числа  $M$  вида  $4n + 3$  (в такой форме можно представить каждое положительное число, если положить  $\mu = 0$ , когда  $M$  нечетно, и  $S = 1$ , когда  $M$  не содержит сомножителей вида  $4n + 3$ ), то  $M$  не может быть разложено на два квадрата, если  $S$  не является квадратом. Если же  $S$  есть квадрат, то имеется  $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$  разложений числа  $M$ , когда хотя бы одно из чисел  $\alpha, \beta, \gamma, \dots$  нечетно, и  $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \dots + \frac{1}{2}$  разложений, когда  $\alpha, \beta, \gamma, \dots$  все четны (речь идет здесь о самих квадратах). Тот, кто сколько-нибудь владеет комбинаторикой, без труда получит доказательство этой теоремы (на котором, как и на других частностях, мы не останавливаемся) из нашей общей теории.

$19 = 1 + 18$ ,  $41 = 9 + 32$ ,  $43 = 25 + 18$ ,  $59 = 9 + 50$ ,  $67 = 49 + 18$ ,  $73 = 1 + 72$ ,  $83 = 81 + 2$ ,  $89 = 81 + 8$ ,  $97 = 25 + 72$  и т. д.

Также и эту теорему, как и многие ей подобные, Ф е р м а знал, хотя доказательство впервые дал Л а г р а н ж, «*Suite des recherches d'Arithmétique*», *Nouv. Mém de l'Ac. de Berlin*, 1775, p. 323 и сл. Многое относящееся к этому предмету исследовал еще Э й л е р, «*Specimen de usu observationum in mathesi pura*», *Comm. nov. Petrop.*, T. VI, p. 185 и сл.; однако полное доказательство теоремы все время не поддавалось его усилиям (ср. также сочинение в T. VIII (1760, 1761 гг.): «*Supplementum quorundam theorematum arithmeticoarum*» в конце).

III. Подобным же путем доказывається, что каждое число, по которому  $-3$  есть квадратичный вычет, может быть представлено или формой  $x^2 + 3y^2$ , или формой  $2x^2 + 2xy + 2y^2$ , и притом так, что значение  $x$  взаимно просто со значением  $y$ . Так как теперь  $-3$  является вычетом всех простых чисел вида  $3n + 1$  (п. 119), а формой  $2x^2 + 2xy + 2y^2$ , очевидно, могут быть представлены только четные числа, мы, как и выше, получаем следующую теорему.

Каждое простое число вида  $3n + 1$  может быть разложено на квадрат и утроенный квадрат, причем только одним единственным способом.

Так, например,  $1 = 1 + 0$ ,  $7 = 4 + 3$ ,  $13 = 1 + 12$ ,  $19 = 16 + 3$ ,  $31 = 4 + 27$ ,  $37 = 25 + 12$ ,  $43 = 16 + 27$ ,  $61 = 49 + 12$ ,  $67 = 64 + 3$ ,  $73 = 25 + 48$  и т. д.

Доказательство этой теоремы впервые дал Э й л е р в упомянутом выше сочинении «*Comm. nov. Petrop.*», T. VIII, p. 105 и сл.

Подобным путем мы могли бы идти и дальше и, например, показать, что каждое простое число вида  $20n + 1$  или  $20n + 3$ , или  $20n + 7$ , или  $20n + 9$  (именно, по которым  $-5$  является вычетом) может быть представлено одной из форм  $x^2 + 5y^2$ ,  $2x^2 + 2xy + 3y^2$ , и притом простые числа вида  $20n + 1$  и  $20n + 9$  — первой, а простые числа вида  $20n + 3$ ,  $20n + 7$  — второй формой; далее, что удвоенные простые числа вида  $20n + 1$ ,  $20n + 9$  могут быть представлены формой  $2x^2 + 2xy + 3y^2$ , а удвоенные простые числа вида  $20n + 3$ ,  $20n + 7$  — формой  $x^2 + 5y^2$ . Однако каждая из этих



теорем и бесчисленное множество других специальных теорем легко могут быть выведены из предыдущего и из того, что будет изложено ниже. Мы переходим поэтому к формам с положительным определителем, и так как их природа совершенно различна в зависимости от того, является ли определитель квадратом или нет, то мы здесь сначала исключим формы с квадратным определителем, а рассмотрим их позднее отдельно.

### О формах с положительным неквадратным определителем

183

**Задача.** Пусть задана любая форма  $(a, b, a')$ , положительный неквадратный определитель которой равен  $D$ ; найти собственно эквивалентную ей форму  $(A, B, C)$ , у которой  $B$  положительно и меньше чем  $\sqrt{D}$ , и, кроме того,  $A$ , если оно положительно, или  $-A$ , если  $A$  отрицательно, лежит между  $\sqrt{D} + B$  и  $\sqrt{D} - B$ .

**Решение.** Мы предположим, что для заданной формы еще не выполняются оба условия, так как иначе нам было бы не нужно искать другую форму. Далее, заметим, что у формы с неквадратным определителем первый или последний член не может быть равен нулю (п. 171, замечание). Пусть  $b' \equiv -b \pmod{a'}$  и расположено между границами  $\sqrt{D}$  и  $\sqrt{D} \mp a'$  (где берется верхний знак, если  $a'$  положительно, и нижний, если оно отрицательно). То, что это возможно, легко доказывается способом, подобным изложенному в п. 3. Положим тогда  $\frac{b'^2 - D}{a'} = a''$ , что является целым числом, так как  $b'^2 - D \equiv b^2 - D \equiv aa' \equiv 0 \pmod{a'}$ . Если теперь  $a'' < a'$ , то пусть снова  $b'' \equiv -b' \pmod{a''}$  и расположено между  $\sqrt{D}$  и  $\sqrt{D} \mp a''$  (в зависимости от того, положительно  $a''$  или отрицательно), и, далее,  $\frac{b''^2 - D}{a''} = a'''$ . Если здесь снова  $a''' < a''$ , то пусть  $b''' \equiv -b'' \pmod{a'''}$  и расположено между  $\sqrt{D}$  и  $\sqrt{D} \mp a'''$ , и  $\frac{b'''^2 - D}{a'''} = a''''$ . Эта операция продолжается до тех пор, пока в ряду чисел  $a', a'', a''', a'''', \dots$  не получится член  $a^{(m+1)}$ , который не меньше, чем предыдущий член  $a^{(m)}$ , что рано или поздно должно случиться, так как иначе мы получили бы бесконечный ряд все

время убывающих целых чисел. Если положить тогда  $a^{(m)} = A$ ,  $b^{(m)} = B$ ,  $a^{(m+1)} = C$ , то форма  $(A, B, C)$  будет удовлетворять всем условиям.

**Доказательство.** I. Так как в ряде форм  $(a, b, a')$ ,  $(a', b', a'')$ ,  $(a'', b'', a''')$ , ... каждая является соседней для предыдущей, последняя,  $(A, B, C)$ , будет собственно эквивалентна первой.

II. Так как  $B$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \mp A$  (где всегда нужно брать верхний знак, если  $A$  положительно, и нижний — если  $A$  отрицательно), то очевидно, что если  $\sqrt{D} - B = p$ ,  $B - (\sqrt{D} \mp A) = q$ , эти величины  $p, q$  будут положительны. Теперь легко устанавливается, что  $q^2 + 2pq + 2p\sqrt{D} = D + A^2 - B^2$ , тем самым  $D + A^2 - B^2$  будет положительным числом, которое мы положим равным  $r$ . Так как  $D = B^2 - AC$ , то  $r = A^2 - AC$ , и потому число  $A^2 - AC$  положительно. Так как, однако, по предположению,  $A$  не больше чем  $C$ , то это, очевидно, может иметь место только в том случае, если  $AC$  отрицательно и потому знаки чисел  $A$  и  $C$  противоположны. Отсюда следует  $B^2 = D + AC < D$  и потому  $B < \sqrt{D}$ .

III. Так как, далее,  $-AC = D - B^2$ , то будет  $AC < D$  и потому (так как  $A$  не больше чем  $C$ )  $A < \sqrt{D}$ . Тем самым  $\sqrt{D} \mp A$  положительно, а значит положительно и  $B$ , которое лежит между границами  $\sqrt{D}$  и  $\sqrt{D} \mp A$ .

IV. Тем самым  $\sqrt{D} + B \mp A$  подавно положительно, и так как  $\sqrt{D} - B \mp A = -q$  отрицательно, то  $\pm A$  лежит между  $\sqrt{D}$  и  $\sqrt{D} - B$ .

**Пример.** Если задана форма  $(67, 97, 140)$ , определитель которой равен 29, то находим ряд форм:  $(67, 97, 140)$ ,  $(140, -97, 67)$ ,  $(67, -37, 20)$ ,  $(20, -3, -1)$ ,  $(-1, 5, 4)$ . Последняя является искомой.

Такие формы  $(A, B, C)$  с положительным определителем  $D$ , у которых  $A$ , взятое положительным, лежит между  $\sqrt{D} + B$  и  $\sqrt{D} - B$ , а  $B$  положительно и меньше чем  $\sqrt{D}$ , мы будем называть приведенными формами. Приведенные формы с положительным неквадратным определителем, таким образом, несколько отличаются от приведенных форм с отрицательным определителем; однако вследствие большой аналогии между теми и другими мы не хотим вводить для них различных названий.

Если бы об эквивалентности двух приведенных форм с положительным определителем можно было судить также легко, как для форм с отрицательным определителем (п. 172), то без труда можно было бы узнавать эквивалентность и двух любых форм с одним и тем же положительным определителем. Однако здесь положение вещей в значительной мере иное, и возможно, что очень многие приведенные формы эквивалентны между собой. Поэтому, прежде чем приступить к этой задаче, мы должны сначала глубже вникнуть в природу приведенных форм (с положительным неквадратным определителем, что мы здесь все время будем предполагать)

1. Если форма  $(a, b, c)$  приведенная, то  $a$  и  $c$  имеют противоположные знаки. Действительно, если определитель формы положить равным  $D$ , то  $ac = b^2 - D$  и потому  $ac$  отрицательно, так как  $b < \sqrt{D}$ .

2. Число  $c$ , так же, как и  $a$ , будучи взято положительным, лежит между  $\sqrt{D} + b$  и  $\sqrt{D} - b$ . Действительно,  $-c = \frac{D - b^2}{a}$ ; поэтому абсолютная величина  $c$  лежит между  $(D - b^2) / (\sqrt{D} + b)$  и  $(D - b^2) / (\sqrt{D} - b)$ , т. е. между  $\sqrt{D} - b$  и  $\sqrt{D} + b$ .

3. Отсюда вытекает, что и форма  $(c, b, a)$  приведенная.

4. Как  $a$ , так и  $c$  меньше, чем  $2\sqrt{D}$ . Именно, каждое из этих чисел меньше, чем  $\sqrt{D} + b$ , и потому подавно меньше, чем  $2\sqrt{D}$ .

5. Число  $b$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \mp a$  (где верхний знак берется при положительном  $a$ , а нижний — при отрицательном  $a$ ). Действительно, так как  $\pm a$  лежит между  $\sqrt{D} + b$  и  $\sqrt{D} - b$ , то  $\pm a - (\sqrt{D} - b)$ , т. е.  $b - (\sqrt{D} \mp a)$  положительно;  $b - \sqrt{D}$ , наоборот, отрицательно; поэтому  $b$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \mp a$ . Точно таким же образом доказывается, что  $b$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \mp c$  (в зависимости от того, положительно  $c$  или отрицательно).

6. Для каждой приведенной формы  $(a, b, c)$  с каждой стороны имеется одна и только одна соседняя приведенная форма. Если  $a' = c$ ,  $b' \equiv -b \pmod{a'}$ , и  $b'$  расположено между  $\sqrt{D}$  и  $\sqrt{D} \mp a'^*$ ,

\* Всюду, где фигурируют двойные знаки, нужно брать верхний, когда  $a'$  положительно, и нижний, когда  $a'$  отрицательно.

далее,  $c = \frac{b'^2 - D}{k'}$ , то форма  $(a', b', c')$  — соседняя справа для формы  $(a, b, c)$ , и одновременно ясно, что если бы была приведена форма, соседняя справа для формы  $(a, b, c)$ , она не могла бы быть отлична от  $(a', b', c')$ . А то, что она действительно приведённая, мы докажем следующим образом.

А. Если положить

$$\sqrt{D} + b \mp a' = p, \quad \pm a' - (\sqrt{D} - b) = q, \quad \sqrt{D} - b = r,$$

то числа  $p, q, r$ , согласно (2) и в силу определения приведённой формы, положительны. Если, далее, положить

$$b' - (\sqrt{D} \mp a') = q', \quad \sqrt{D} - b' = r',$$

то числа  $q', r'$  положительны, так как  $b'$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \mp a'$ . Наконец, если  $b + b' = \pm ma'$ , то  $m$  — целое число. Теперь очевидно, что  $p + q' = b + b'$ , и потому  $b + b'$ , т. е.  $\pm ma'$ , а, значит, и  $m$  положительны. Отсюда следует, что  $m - 1$  заведомо не отрицательно. Далее,

$$r + q' \pm ma' = 2b' \pm a', \quad \text{т. е.} \quad 2b' = r + q' \pm (m - 1)a',$$

и потому  $2b'$  и  $b'$  обязательно положительны; и так как  $b' + r' = \sqrt{D}$ , то  $b' < \sqrt{D}$ .

В. Далее,

$$r \pm ma' = \sqrt{D} + b', \quad \text{т. е.} \quad r \pm (m - 1)a' = \sqrt{D} + b' \mp a',$$

и потому  $\sqrt{D} + b' \mp a'$  положительно. Из этого и из того, что  $\pm a' - (\sqrt{D} - b') = q'$  и потому положительно, следует, что  $\pm a'$  лежит между  $\sqrt{D} + b'$  и  $\sqrt{D} - b'$ . Поэтому форма  $(a', b', c')$  приведённая.

Таким же образом доказывается, что если  $'c = a$ ,  $'b \equiv -b \pmod{'c}$  и  $'b$  лежит между  $\sqrt{D}$  и  $\sqrt{D} \pm 'c$ , далее,  $'a = \frac{'b^2 - D}{'c}$ , то форма  $(a', b', c')$  приведённая. Но очевидно, что эта форма является соседней слева для формы  $(a, b, c)$ , и никакая другая приведённая форма, кроме  $(a', b', c')$ , этим свойством обладать не может.

**Пример.** Для приведенной формы  $(5, 11, -14)$ , определитель которой равен 191, соседней справа является приведенная форма  $(-14, 3, 13)$ , а соседней слева — форма  $(-22, 9, 5)$ .

7. Если приведенная форма  $(a', b', c')$  является соседней справа для приведенной формы  $(a, b, c)$ , то для приведенной формы  $(c, b, a)$  форма  $(c', b', a')$  будет соседней слева; и если для приведенной формы  $(a, b, c)$  форма  $(a', b', c')$  является соседней слева, то приведенная форма  $(c', b', a')$  будет для приведенной формы  $(c, b, a)$  соседней справа. Далее, формы  $(-a', b', -c')$ ,  $(-a, b, -c)$ ,  $(-a', b, -c')$  также будут приведенными, причем вторая для первой и третья для второй являются соседними справа, или первая для второй и вторая для третьей — соседними слева, и подобным же образом обстоит дело с тремя формами  $(-c', b', -a')$ ,  $(-c, b, -a)$ ,  $(-c', b, -a)$ . Это настолько ясно, что не требует пояснения.

## 185

*Количество всех приведенных форм с данным определителем  $D$  всегда конечно; сами же они могут быть найдены двумя способами. Мы будем обозначать произвольные приведенные формы с определителем  $D$  через  $(a, b, c)$ , так что должны быть определены все значения  $a, b, c$ .*

**Первый метод.** Будем брать за  $a$  все числа (как положительные, так и отрицательные), которые меньше чем  $2\sqrt{D}$  и по которым  $D$  является квадратичным вычетом, и для каждого отдельного  $a$  будем полагать число  $b$  равным всевозможным положительным значениям выражения  $\sqrt{D} \pmod{a}$ , которые лежат между  $\sqrt{D}$  и  $\sqrt{D} \mp a$ , а  $c$  для отдельных значений  $a, b$  будем полагать равным  $(b^2 - D)/a$ . Если при этом получатся какие-нибудь формы, у которых  $\pm a$  лежит вне интервала  $\sqrt{D} + b$  и  $\sqrt{D} - b$ , то их нужно выбросить.

**Второй метод.** За  $b$  берутся все положительные числа, которые меньше чем  $\sqrt{D}$ , для отдельных  $b$  выражение  $b^2 - D$  разлагается всеми возможными способами на два сомножителя, которые, будучи взятыми по абсолютной величине, лежат между  $\sqrt{D} + b$  и  $\sqrt{D} - b$ . и один из них полагается равным  $a$ , а другой равным  $c$ . Очевид-

но, что каждое отдельное разложение на сомножители дает две формы, потому что каждый из сомножителей должен быть положен равным как  $a$ , так и  $c$ .

**Пример.** Если  $D = 79$ , то значения  $a$  будут следующими двадцатью двумя:  $\mp 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15$ . Отсюда находим девятнадцать форм:

$(1, 8, -15), (2, 7, -15), (3, 8, -5), (3, 7, -10), (5, 8, -3),$   
 $(5, 7, -6), (6, 7, -5), (6, 5, -9), (7, 4, -9), (7, 3, -10),$   
 $(9, 5, -6), (9, 4, -7), (10, 7, -3), (10, 3, -7), (13, 1, -6),$   
 $(14, 3, -5), (15, 8, -1), (15, 7, -2), (15, 2, -5),$

и столько же других, которые получаются из этих, если меняются знаки крайних членов, именно, формы  $(-1, 8, 15), (-2, 7, 15), \dots$ , так что всего форм имеется тридцать восемь. Из них, однако, шесть должны быть выброшены, именно,  $(\pm 13, 1, \mp 6), (\pm 14, 3, \mp 5), (\pm 15, 2, \mp 5)$ ; остальные тридцать две охватывают все приведенные формы. Вторым методом эти же формы получаются в следующем порядке\*:

$(\pm 7, 3, \mp 10), (\pm 10, 3, \mp 7), (\pm 7, 4, \mp 9), (\pm 9, 4, \mp 7),$   
 $(\pm 6, 5, \mp 9), (\pm 9, 5, \mp 6), (\pm 2, 7, \mp 15), (\pm 3, 7, \mp 10),$   
 $(\pm 5, 7, \mp 6), (\pm 6, 7, \mp 5), (\pm 10, 7, \mp 3), (\pm 15, 7, \mp 2),$   
 $(\pm 1, 8, \mp 15), (\pm 3, 8, \mp 5), (\pm 5, 8, \mp 3), (\pm 15, 8, \mp 1).$

Пусть  $F$  приведенная форма с определителем  $D$ , и для нее форма  $F'$  является соседней справа, для  $F'$  форма  $F''$  является соседней справа, для  $F''$  форма  $F'''$  является соседней справа и т. д. Тогда, очевидно, все формы  $F', F'', F''', \dots$  являются вполне определенными и собственно эквивалентными как между собой, так и форме  $F$ . Так как, однако, число всех при-

---

\* При  $b = 1$  число  $-78$  не может быть разложено на два сомножителя, абсолютные величины которых лежат между  $\sqrt{79} + 1$  и  $\sqrt{79} - 1$ ; вследствие этого указанное значение, а по аналогичной причине и значения 2 и 6, нужно отбросить.

веденных форм с заданным определителем конечно, то ясно, что в бесконечном ряду  $F, F', F'', \dots$  не все формы могут быть различными между собой. Если предположить, что  $F^{(m)}$  и  $F^{(m+n)}$  совпадают, то  $F^{(m-1)}$  и  $F^{(m+n-1)}$  будут приведенными, соседними слева для одной и той же приведенной формы и потому будут совпадать, поэтому  $F^{(m-2)}$  и  $F^{(m+n-2)}$  и т. д., наконец,  $F$  и  $F^{(n)}$  тоже будут совпадать. Следовательно, в ряду  $F, F', F'', \dots$ , если только он продолжен достаточно далеко, обязательно повторится первая форма  $F$ , и если мы предположим, что  $F^{(n)}$  — первая форма, совпадающая с  $F$ , или что  $F', F'', \dots, F^{(n-1)}$  все отличны от  $F$ , то легко видеть, что все формы  $F, F', F'', \dots, F^{(n-1)}$  различны между собой. Совокупность этих форм мы будем называть периодом формы  $F$ . Если поэтому ряд будет продолжаться дальше последней формы периода, то все время будут снова повторяться формы  $F, F', F'', \dots$ , и весь бесконечный ряд будет образован из этого бесконечно много раз повторяющегося периода формы  $F$ .

Ряд  $F, F', F'', \dots$  может быть продолжен и в обратную сторону, если перед формой  $F$  поставить приведенную форму  $'F$ , которая является для нее соседней слева, перед  $'F$  — форму  $''F$ , которая является для нее соседней слева, и т. д. При этом получается бесконечный в обе стороны ряд форм

$$\dots, ''F, 'F, F, F', F'', F''', \dots,$$

и легко видеть, что  $'F$  совпадает с  $F^{(n-1)}$ ,  $''F$  совпадает с  $F^{(n-2)}$  и т. д., и потому ряд и влево составляется из бесконечное число раз повторяющегося периода формы  $F$ .

Если формам  $F, F', F'', \dots, 'F, ''F, \dots$  придать соответственно индексы  $0, 1, 2, \dots, -1, -2, \dots$ , и вообще форме  $F^{(m)}$  — индекс  $m$ , а форме  ${}^{(m)}F$  — индекс  $-m$ , то очевидно, что две формы ряда будут совпадающими или различными в зависимости от того, сравнимы по модулю  $n$  их индексы или нет.

**Пример.** В качестве периода формы  $(3, 8, -5)$ , определитель которой равен 79, получается ряд  $(3, 8, -5), (-5, 7, 6), (6, 5, -9), (-9, 4, 7), (7, 3, -10), (-10, 7, 3)$ . После последней формы снова получается  $(3, 8, -5)$ . Таким образом, здесь  $n = 6$ .

Сейчас мы дадим несколько общих замечаний об этих периодах.

1. Если формы  $F, F', F'', \dots, 'F, ''F, ''''F, \dots$  представлены следующим образом:

$$(a, b, -a'), (-a', b', a''), (a'', b'', -a'''), \dots, (-'a, 'b, 'c),$$

$$(''a, ''b, -'a), (-'''a, '''b, ''a), \dots,$$

то все величины  $a, a', a'', a''', \dots, 'a, ''a, ''''a, \dots$  будут иметь одинаковые знаки (п. 184,1),  $a, b, b', b'', \dots, 'b, ''b, \dots$  все будут положительны.

2. Отсюда вытекает, что число  $n$  (количество форм, из которых состоит период формы  $F$ ) всегда четно. Действительно, первый член какой-нибудь формы  $F^{(m)}$  из этого периода будет, очевидно, обладать тем же знаком, что и первый член  $a$  формы  $F$ , если  $m$  четно, и противоположным, если  $m$  нечетно. Поэтому, так как  $F^{(n)}$  и  $F$  совпадают,  $n$  обязательно будет четным.

3. Алгоритм, при помощи которого отыскиваются числа  $b', b'', b''', \dots, a'', a''', \dots$ , согласно п. 184,6, состоит в следующем:

$$\begin{aligned} b' &\equiv -b \pmod{a'} && \text{между границами } \sqrt{D} \text{ и } \sqrt{D} \mp a'; && a'' = \frac{D - b'^2}{a'}; \\ b'' &\equiv -b' \pmod{a''} && \text{» } \sqrt{D} \text{ и } \sqrt{D} \mp a''; && a''' = \frac{D - b''^2}{a''}; \\ b''' &\equiv -b'' \pmod{a'''} && \text{» } \sqrt{D} \text{ и } \sqrt{D} \mp a'''; && a'''' = \frac{D - b'''^2}{a'''}, \end{aligned}$$

причем во втором столбце нужно брать верхний или нижний знак в зависимости от того, положительны  $a, a', a'', \dots$  или отрицательны. Вместо формул в третьем столбце можно взять и следующие, которые удобнее, когда число  $D$  большое:

$$\begin{aligned} a'' &= \frac{b + b'}{a'} (b - b') + a, \\ a''' &= \frac{b' + b''}{a''} (b' - b'') + a', \\ a'''' &= \frac{b'' + b'''}{a'''} (b'' - b''') + a'' \end{aligned}$$

и т. д.



4. Каждая форма  $F^{(m)}$ , которая содержится в периоде формы  $F$ , будет по сути дела иметь тот же период, что и  $F$ . Именно, этот период будет таков:  $F^{(m)}$ ,  $F^{(m+1)}$ , ...,  $F^{(n-1)}$ ,  $F$ ,  $F'$ , ...,  $F^{(m-1)}$ ; в нем встречаются те же формы и в том же порядке, что и в периоде формы  $F$ , и он отличается от последнего только в отношении своего начала и конца.

5. Отсюда следует, что все приведенные формы с одинаковым определителем  $D$  могут быть разбиты на периоды. Берется по желанию любая такая форма  $F$  и отыскивается ее период  $F, F', F'', \dots, F^{(n-1)}$ , который можно обозначить через  $P$ . Если он еще не охватывает всех приведенных форм с определителем  $D$ , то пусть какая-нибудь не содержащаяся в нем форма есть  $G$ , а ее период есть  $Q$ . Тогда ясно, что  $P$  и  $Q$  не могут иметь общих форм, так как иначе и  $G$  должна была бы содержаться в  $P$ , и периоды вообще совпадали бы. Если  $P$  и  $Q$  еще не исчерпывают всех приведенных форм, то не входящая туда форма  $H$  даст третий период  $R$ , который не имеет общих форм ни с  $P$ , ни с  $Q$ . Таким способом можно поступать, пока не исчерпаются все приведенные формы. Так, например, все приведенные формы с определителем 79 разбиваются на шесть периодов:

I. (1, 8, — 15), (—15, 7, 2), (2, 7, —15), (—15, 8, 1).

II. (—1, 8, 15), (15, 7, —2), (—2, 7, 15), (15, 8, —1).

III. (3, 8, —5), (—5, 7, 6), (6, 5, —9), (—9, 4, 7), (7, 3, —10), (—10, 7, 3).

IV. (—3, 8, 5), (5, 7, —6), (—6, 5, 9), (9, 4, —7), (—7, 3, 10), (10, 7, —3).

V. (5, 8, —3), (—3, 7, 10), (10, 3, —7), (—7, 4, 9), (9, 5, —6), (—6, 7, 5).

VI. (—5, 8, 3), (3, 7, —10), (—10, 3, 7), (7, 4, —9), (—9, 5, 6), (6, 7, —5).

6. Мы будем называть ассоциированными формами такие формы, которые состоят из одних и тех же, но стоящих в противоположном порядке, членов, например,  $(a, b, -a')$ ,  $(-a', b, a)$ . Тогда из п. 184,7 легко видно, что если приведенная форма  $F$  имеет период  $F, F', F'', \dots, F^{(n-1)}$ , далее, с формой  $F$  ассоциирована форма  $f$  и с формами  $F^{(n-1)}, F^{(n-2)}, \dots, F'', F'$  — соответственно формы  $f', f'', \dots, f^{(n-2)}, f^{(n-1)}$ , то периодом формы  $f$  будет

$f, f', f'', \dots, f^{(n-2)}, f^{(n-1)}$ , и потому он будет состоять из стольких же форм, что и период формы  $F$ . Периоды ассоциированных форм мы будем называть ассоциированными периодами. Так, в нашем примере ассоциированы периоды III и VI и точно так же IV и V.

7. Возможно, однако, и то, что форма  $f$  сама содержится в периоде ассоциированной с ней формы  $F$  как в нашем примере обстоит дело для периодов I и II, и что тем самым период формы  $F$  совпадает с периодом формы  $f$  или, что период формы  $F$  ассоциирован с самим собой. Если это имеет место, то в таком периоде встречаются две двусторонние формы. Именно, если мы предположим, что период формы  $F$  состоит из  $2n$  форм, или что  $F$  и  $F^{(2n)}$  совпадают, и если, далее, индекс формы  $f$  в периоде формы  $F$  равен  $2m + 1$  \*, т. е.  $F^{(2m+1)}$  и  $F$  ассоциированы, то очевидно, что ассоциированы также  $F'$  и  $F^{(2m)}$ ,  $F''$  и  $F^{(2m-1)}$  и т. д., и потому также  $F^{(m)}$  и  $F^{(m+1)}$ . Если  $F^{(m)} = (a^{(m)}, b^{(m)}, -a^{(m+1)})$ ,  $F^{(m+1)} = (-a^{(m+1)}, b^{(m+1)}, a^{(m+2)})$ , то  $b^{(m)} + b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$ ; но по определению ассоциированных форм,  $b^{(m)} = b^{(m+1)}$  и тем самым  $2b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$ , т. е. форма  $F^{(m+1)}$  — двусторонняя. Точно так же ассоциированы  $F^{(2m+1)}$  и  $F^{(2n)}$ , поэтому — также  $F^{(2m+2)}$  и  $F^{(2n-1)}$ , далее,  $F^{(2m+3)}$  и  $F^{(2n-2)}$  и т. д., и, наконец,  $F^{(m+n)}$  и  $F^{(m+n+1)}$ ; последняя из этих форм является, однако, двусторонней, что легко доказывается подобным же рассуждением. Но так как  $m + 1$  и  $m + n + 1$  по модулю  $2n$  не сравнимы, формы  $F^{(m+1)}$  и  $F^{(m+n+1)}$  не совпадают (п. 186, где  $n$  обозначает то же самое, что здесь  $2n$ ). Так, в нашем примере в I находятся двусторонние формы  $(1, 8, -15)$ ,  $(2, 7, -15)$ , в II — формы  $(-1, 8, 15)$ ,  $(-2, 7, 15)$ .

8. Обратно, каждый период, в котором имеется двусторонняя форма, ассоциирован с самим собой. Действительно, легко видеть, что если  $F^{(m)}$  есть приведенная двусторонняя форма, то ассоциированная с ней форма (которая тоже является приведенной) будет одновременно для нее соседней слева, т. е. формы  $F^{(m-1)}$  и  $F^{(m)}$

\* Индекс здесь обязательно будет нечетным, так как первые члены форм  $F, f$ , очевидно, имеют противоположные знаки (ср. выше, п. 187, 2).

ассоциированы. Тогда, однако, весь период ассоциирован с самим собой. Отсюда вытекает, что *не может быть, чтобы в каком-нибудь периоде содержалась только одна единственная двусторонняя форма.*

9. Однако в одном и том же периоде их не может быть и больше двух. Именно, если мы предположим, что в состоящем из  $2n$  форм периоде формы  $F$  имеется три двусторонних формы  $F^{(\lambda)}$ ,  $F^{(\mu)}$ ,  $F^{(\nu)}$ , которые принадлежат соответственно индексам  $\lambda$ ,  $\mu$ ,  $\nu$ , так что числа  $\lambda$ ,  $\mu$ ,  $\nu$  — неравные, лежащие в границах от 0 до  $2n - 1$  (включительно), то будут ассоциированными формы  $F^{(\lambda-1)}$  и  $F^{(\lambda)}$ , и точно так же  $F^{(\lambda-2)}$  и  $F^{(\lambda+1)}$  и т. д., и, наконец,  $F$  и  $F^{(2\lambda-1)}$ . На том же основании ассоциированы  $F$  и  $F^{(2\mu-1)}$ , так же, как  $F$  и  $F^{(2\nu-1)}$ . Поэтому  $F^{(2\lambda-1)}$ ,  $F^{(2\mu-1)}$ ,  $F^{(2\nu-1)}$  совпадают и индексы  $2\lambda - 1$ ,  $2\mu - 1$ ,  $2\nu - 1$  сравнимы по модулю  $2n$ , а значит, и  $\lambda \equiv \mu \equiv \nu \pmod{n}$ . Это, однако, невозможно, так как между границами 0 и  $2n - 1$ , очевидно, не могут лежать три различных сравнимых по модулю  $n$  числа.

## 188

Так как все формы из одного и того же периода собственно эквивалентны, возникает вопрос, *могут ли быть также собственно эквивалентными и формы из различных периодов.* Однако прежде чем показать, что это невозможно, мы должны изложить кое-что относительно преобразований приведенных форм.

Так как в дальнейшем мы очень часто должны будем иметь дело с преобразованием форм, то чтобы, насколько это возможно, избежать длиннот, мы, начиная с этого места, все время будем пользоваться следующим сокращенным способом записи. Если форма  $LX^2 + 2MXY + NY^2$  подстановкой  $X = \alpha x + \beta y$ ,  $Y = \gamma x + \delta y$  преобразуется в форму  $lx^2 + 2txy + ny^2$ , мы будем говорить просто, что  $(L, M, N)$  переходит при подстановке  $\alpha, \beta, \gamma, \delta$  в  $(l, t, n)$ . При этом не нужно будет специально обозначать неизвестные форм, о которых идет речь. Однако, очевидно, что в каждой форме следует различать *первую* неизвестную от *второй*.

Пусть задана приведенная форма  $(a, b, -a')$  с определителем  $D$ . Образует аналогично тому, как в п. 186, уходящий в обе

стороны в бесконечность ряд приведенных форм  $\dots, {}''f, {}'f, f, f', f'', \dots$ , причем пусть

$$f' = (-a', b', a''), f'' = (a'', b'', -a'''), \dots, \\ {}'f = (-{}'a, {}'b, a), {}''f = ({}''a, {}''b, -{}'a), \dots$$

Если положить

$$\frac{b+b'}{-a'} = h', \frac{b'+b''}{a''} = h'', \frac{b''+b'''}{-a'''} = h''', \dots, \\ \frac{{}'b+b}{a} = h, \frac{{}''b+{}'b}{-{}'a} = {}'h, \frac{{}'''b+{}''b}{{}''a} = {}''h, \dots,$$

то, очевидно, что если мы (как в п. 177) образуем числа  $\alpha', \alpha'', \alpha''', \dots, \beta', \beta'', \beta''', \dots$  и т. д. по алгоритму

$$\begin{aligned} \alpha' &= 0, & \beta' &= -1, & \gamma' &= 1, & \delta' &= h', \\ \alpha'' &= \beta', & \beta'' &= h''\beta', & \gamma'' &= \delta', & \delta'' &= h''\delta' - 1, \\ \alpha''' &= \beta'', & \beta''' &= h'''\beta'' - \beta', & \gamma''' &= \delta'', & \delta''' &= h'''\delta'' - \delta', \\ \alpha'''' &= \beta''', & \beta'''' &= h''''\beta''' - \beta'', & \gamma'''' &= \delta''', & \delta'''' &= h''''\delta''' - \delta'', \\ & & & & & & & \text{и т. д.}, \end{aligned}$$

то  $f$  будет переходить в

$$\begin{aligned} f' & \text{ при подстановке } \alpha', \beta', \gamma', \delta', \\ f'' & \text{ » » } \alpha'', \beta'', \gamma'', \delta'', \\ f''' & \text{ » » } \alpha''', \beta''', \gamma''', \delta''', \\ & \text{и т. д.}, \end{aligned}$$

и все эти преобразования будут собственными.

Так как  $'f$  переходит в  $f$  при собственной подстановке  $0, -1, 1, h$  (п. 158),  $f$  будет переходить в  $'f$  при собственной подстановке  $h, 1, -1, 0$ . По аналогичной причине  $'f$  будет переходить в  $''f$  при собственной подстановке  $'h, 1, -1, 0$ ,  $''f$  в  $'''f$  при собственной подстановке  ${}''h, 1, -1, 0$  и т. д. Отсюда, в соответствии с п. 159, тем же способом, как в п. 177, можно вывести, что если числа  $'\alpha, {}''\alpha, {}'''\alpha, \dots, {}'\beta, {}''\beta, {}'''\beta, \dots$  и т. д. образуются по следующему алгоритму:

$$\begin{aligned} {}'\alpha &= h, & {}'\beta &= 1, & {}'\gamma &= -1, & {}'\delta &= 0, \\ {}''\alpha &= {}'h {}'\alpha - 1, & {}''\beta &= {}'\alpha, & {}''\gamma &= {}'h {}'\gamma, & {}''\delta &= {}'\gamma, \end{aligned}$$

$$\begin{aligned}''' \alpha &= {}''h'' \alpha - {}' \alpha, &''' \beta &= {}'' \alpha, &''' \gamma &= {}''h'' \gamma - {}' \gamma, &''' \delta &= {}'' \gamma, \\''' \alpha &= {}'''h''' \alpha - {}'' \alpha, &''' \beta &= {}''' \alpha, &''' \gamma &= {}'''h''' \gamma - {}'' \gamma, &''' \delta &= {}''' \gamma,\end{aligned}$$

и т. д.,

то  $f$  переходит в

$$\begin{aligned}' f &\text{ при подстановке } {}' \alpha, {}' \beta, {}' \gamma, {}' \delta, \\'' f &\text{ » » } {}'' \alpha, {}'' \beta, {}'' \gamma, {}'' \delta, \\''' f &\text{ » » } {}''' \alpha, {}''' \beta, {}''' \gamma, {}''' \delta,\end{aligned}$$

и т. д.,

и что все эти преобразования собственные.

Если положить  $\alpha = 1$ ,  $\beta = 0$ ,  $\gamma = 0$ ,  $\delta = 1$ , то эти числа будут иметь для формы  $f$  то же значение, что и числа  $\alpha'$ ,  $\beta'$ ,  $\gamma'$ ,  $\delta'$  для  $f'$ ;  $\alpha''$ ,  $\beta''$ ,  $\gamma''$ ,  $\delta''$  для  $f''$ , и т. д.;  $'\alpha$ ,  $'\beta$ ,  $'\gamma$ ,  $'\delta$  для  $'f$ , и т. д. Именно, при подстановке  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$  форма  $f$  переходит в  $f$ . Но тогда бесконечные ряды  $\alpha'$ ,  $\alpha''$ ,  $\alpha'''$ , . . . ,  $'\alpha$ ,  $''\alpha$ ,  $''' \alpha$ , . . . посредством вставки члена  $\alpha$  приводятся в такую тесную связь, что они могут рассматриваться как один связанный бесконечный в обе стороны ряд, который все время строится по одному и тому же закону: . . . ,  $''' \alpha$ ,  $''\alpha$ ,  $'\alpha$ ,  $\alpha$ ,  $\alpha'$ ,  $\alpha''$ ,  $\alpha'''$ , . . . Закон построения следующий:

$$\begin{aligned}''' \alpha + {}' \alpha &= {}''h'' \alpha, &'' \alpha + \alpha &= {}'h' \alpha, &' \alpha + \alpha' &= h \alpha, \\ \alpha + \alpha'' &= h' \alpha', &\alpha' + \alpha''' &= h'' \alpha'', &\dots\end{aligned}$$

или, вообще (если считать, что отрицательный индекс, добавленный справа, обозначает то же, что положительный индекс, добавленный слева),

$$\alpha^{(m-1)} + \alpha^{(m+1)} = h^{(m)} \alpha^{(m)}.$$

Аналогично является непрерывно связанным ряд . . . ,  $''\beta$ ,  $'\beta$ ,  $\beta$ ,  $\beta'$ ,  $\beta''$ , . . . , законом построения которого является

$$\beta^{(m-1)} + \beta^{(m+1)} = h^{(m+1)} \beta^{(m)},$$

и этот ряд будет совпадать с предыдущим, если все члены сдвинуты на одно место:  $''\beta = {}' \alpha$ ,  $'\beta = \alpha$ ,  $\beta = \alpha'$  и т. д. Закон построения непрерывного ряда . . . ,  $''\gamma$ ,  $'\gamma$ ,  $\gamma$ ,  $\gamma'$ ,  $\gamma''$ , . . . следующий:

$$\gamma^{(m-1)} + \gamma^{(m+1)} = h^{(m)} \gamma^{(m)},$$

и законом построения ряда . . . , " $\delta$ , ' $\delta$   $\delta$ ,  $\delta'$ ,  $\delta''$ , . . . будет

$$\delta^{(m-1)} + \delta^{(m+1)} = h^{(m+1)} \delta^{(m)},$$

и, кроме того, вообще,

$$\delta^{(m)} = \gamma^{(m+1)}.$$

**Пример.** Если заданная форма есть  $f = (3, 8, -5)$ , то она будет преобразовываться

|         |                       |              |                          |
|---------|-----------------------|--------------|--------------------------|
| в форму | $''''f = (-10, 7, 3)$ | подстановкой | $-805, -152, +143, +27,$ |
| »       | $''''f = (3, 8, -5)$  | »            | $-152, +45, +27, -8,$    |
| »       | $'''f = (-5, 7, 6)$   | »            | $+45, +17, -8, -3,$      |
| »       | $''f = (6, 5, -9)$    | »            | $+17, -11, -3, +2,$      |
| »       | $'f = (-9, 4, 7)$     | »            | $-11, -6, +2, +1,$       |
| »       | $f = (7, 3, -10)$     | »            | $-6, +5, +1, -1,$        |
| »       | $'f = (-10, 7, 3)$    | »            | $+5, +1, -1, 0,$         |
| »       | $f = (3, 8, -5)$      | »            | $+1, 0, 0, +1,$          |
| »       | $f' = (-5, 7, 6)$     | »            | $0, -1, +1, -3,$         |
| »       | $f'' = (6, 5, -9)$    | »            | $-1, -2, -3, -7,$        |
| »       | $f''' = (-9, 4, 7)$   | »            | $-2, +3, -7, +10,$       |
| »       | $f'''' = (7, 3, -10)$ | »            | $+3, +5, +10, +17,$      |
| »       | $f'''' = (-10, 7, 3)$ | »            | $+5, -8, +17, -27,$      |
| »       | $f'''' = (3, 8, -5)$  | »            | $-8, -45, -27, -152,$    |
| »       | $f'''' = (-5, 7, 6)$  | »            | $-45, +143, -152, +483,$ |

и т. д.

*Относительно этого алгоритма нужно заметить следующее.*

1. Все числа  $a, a', a'', \dots, 'a, ''a, \dots$  имеют одинаковые знаки; все числа  $b, b', b'', \dots, 'b, ''b, \dots$  положительны. В ряду . . . " $h, 'h, h, h', h'', \dots$  знаки чередуются: именно, если все числа  $a, a', \dots$  положительны, то  $h^{(m)}$  или  ${}^{(m)}h$  будут положительны при четном  $m$  и отрицательны при нечетном  $m$ ; если же  $a, a', \dots$  отрицательны, то  $h^{(m)}$  или  ${}^{(m)}h$  будут отрицательны при четном  $m$  и положительны при нечетном  $m$ .

2. Если  $a$  положительно и потому  $h'$  отрицательно,  $h''$  положительно и т. д., то  $\alpha'' = -1$  отрицательно,  $\alpha''' = h'' \alpha''$  отрицательно и по абсолютной величине больше чем  $\alpha''$  (или равно  $\alpha''$ , если  $h'' = 1$ );  $\alpha'''' = h''' \alpha''' - \alpha''$  положительно и по абсолютной величине больше чем  $\alpha'''$  (потому что  $h''' \alpha'''$  положительно,  $\alpha''$  отрицательно);  $\alpha''''' = h'''' \alpha'''' - \alpha'''$  положительно и по абсолютной величине больше чем  $\alpha''''$  (потому что  $h'''' \alpha''''$  положительно) и т. д. Отсюда легко видеть, что ряд  $\alpha', \alpha'', \alpha''', \dots$  возрастает до бесконечности и что все время два положительных знака чередуются с двумя отрицательными, так что  $\alpha^{(m)}$  имеет знак  $+$ ,  $+$ ,  $-$ ,  $-$ , если соответственно  $m \equiv 0, 1, 2, 3 \pmod{4}$ . Если  $a$  отрицательно, то подобной же последовательностью рассуждений находим, что  $\alpha''$  отрицательно,  $\alpha'''$  положительно и по абсолютной величине или больше чем  $\alpha''$ , или равно  $\alpha''$ ;  $\alpha''''$  положительно и больше чем  $\alpha'''$ ;  $\alpha'''''$  отрицательно и по абсолютной величине больше чем  $\alpha''''$  и т. д., так что ряд  $\alpha', \alpha'', \alpha''', \dots$  все время возрастает, и знак члена  $\alpha^{(m)}$  есть  $+$ ,  $-$ ,  $-$ ,  $+$  если соответственно  $m \equiv 0, 1, 2, 3 \pmod{4}$ .

3. Таким же способом находим, что все четыре бесконечных ряда  $\alpha', \alpha'', \alpha''', \dots, \gamma, \gamma', \gamma'', \dots, \alpha', \alpha, ' \alpha, '' \alpha, \dots, \gamma, ' \gamma, '' \gamma, \dots$ , а потому и следующие, идентичные с ними ряды  $\beta, \beta', \beta'', \dots, ' \delta, \delta, \delta', \delta'', \dots, \beta, ' \beta, '' \beta, \dots, ' \delta, '' \delta, \dots$  непрерывно возрастают, и в зависимости от того, имеет ли место  $m \equiv 0, 1, 2, 3 \pmod{4}$ , знаки таковы:

$$\begin{array}{ll} \text{у } \alpha^{(m)} & +, \pm, -, \mp, & \text{у } \beta^{(m)} & \pm, -, \mp, +, \\ \text{у } \gamma^{(m)} & \pm, +, \mp, -, & \text{у } \delta^{(m)} & +, \mp, -, \pm, \\ \text{у } {}^{(m)}\alpha & +, \pm, -, \mp, & \text{у } {}^{(m)}\beta & \mp, +, \pm, -, \\ \text{у } {}^{(m)}\gamma & \mp, -, \pm, +, & \text{у } {}^{(m)}\delta & +, \mp, -, \pm, \end{array}$$

где следует брать верхний знак, если  $a$  положительно, и нижний, если  $a$  отрицательно. В частности, можно было бы отметить следующее свойство. Если  $m$  обозначает какой-нибудь положительный индекс, то  $\alpha^{(m)}$  и  $\gamma^{(m)}$  будут иметь одинаковые знаки, если  $a$  положительно, и противоположные, если  $a$  отрицательно, и аналогично обстоит дело для  $\beta^{(m)}$  и  $\delta^{(m)}$ ; наоборот,  ${}^{(m)}\alpha$  и  ${}^{(m)}\gamma$  или  ${}^{(m)}\beta$  и  ${}^{(m)}\delta$  будут иметь одинаковые знаки, если  $a$  отрицательно, и противоположные, если  $a$  положительно.

4. В обозначениях п. 27 величины  $\alpha^{(m)}, \dots$  коротко могут быть выражены следующим образом. Если положить

$$\mp h' = k', \quad \pm h'' = k'', \quad \mp h''' = k''', \quad \dots,$$

$$\dots, \quad \pm h = k, \quad \mp' h = 'k, \quad \pm'' h = ''k, \quad \dots,$$

так что все числа  $k', k'', \dots, k, 'k, \dots$  положительны, то

$$\begin{aligned} \alpha^{(m)} &= \pm [k'', k''', k''', \dots, k^{(m-1)}], & \beta^{(m)} &= \pm [k'', k''', k''', \dots, k^{(m)}], \\ \gamma^{(m)} &= \pm [k', k'', k''', \dots, k^{(m-1)}]; & \delta^{(m)} &= \pm [k', k'', k''', \dots, k^{(m)}], \\ {}^{(m)}\alpha &= \pm [k, 'k, ''k, \dots, {}^{(m-1)}k], & {}^{(m)}\beta &= \pm [k, 'k, ''k, \dots, {}^{(m-2)}k], \\ {}^{(m)}\gamma &= \pm ['k, ''k, ''''k, \dots, {}^{(m-1)}k], & {}^{(m)}\delta &= \pm ['k, ''k, ''''k, \dots, {}^{(m-2)}k], \end{aligned}$$

причем знаки должны определяться по указанным выше правилам. По этим формулам, доказательство которых мы, вследствие их легкости, опускаем, вычисления всегда могут быть проведены кратчайшим образом.

## 190

**Лемма.** Если  $t, \mu, t', n, \nu, n'$  обозначают какие-нибудь целые числа, однако такие, что из трех последних ни одно не равно нулю, то я утверждаю, что если  $\mu/\nu$  лежит между границами  $t/n$  и  $t'/n'$  (которые сами исключаются), и  $tn' - nt' = \pm 1$ , то знаменатель  $\nu$  будет больше, чем  $n$  и  $n'$ .

**Доказательство.** Очевидно, что  $\mu n n'$  лежит между  $\nu t n'$  и  $\nu n t'$ , и потому отличается от обеих границ меньше, чем одна граница отличается от другой, т. е.  $\nu t n' - \nu n t' > \mu n n' - \nu t n'$  и  $> \mu n n' - - \nu n t'$ , или  $\nu > n' (\mu n - \nu t)$  и  $> n (\mu n' - \nu t')$ . Отсюда следует, что так как  $\mu n - \nu t$ , очевидно, не равно 0 (ибо в противном случае, вопреки предположению, было бы  $\frac{\mu}{\nu} = \frac{t}{n}$ ) и также  $\mu n' - \nu t'$  не равно 0 (по аналогичной причине), каждое из этих выражений равно 1,  $\nu > n'$  и  $\nu > n$ .

Поэтому ясно, что  $\nu$  не может быть равно 1, т. е. что если  $tn' - nt' = \pm 1$ , то между дробями  $t/n$ ,  $t'/n'$  не может лежать целое число. Поэтому между ними не может лежать и нуль, т. е. указанные дроби не могут иметь противоположных знаков.



**Теорема.** Если приведенная форма  $(a, b, -a')$  с определителем  $D$  переводится подстановкой  $\alpha, \beta, \gamma, \delta$  в приведенную форму  $(A, B, -A')$  с тем же определителем, то, во-первых,  $(\pm \sqrt{D} - b)/a$  лежит между  $\alpha/\gamma$  и  $\beta/\delta$  (если ни  $\gamma$ , ни  $\delta$  не равны нулю, т. е. если обе границы конечны), причем верхний знак нужно брать тогда, когда ни одна из обеих границ не имеет знака, противоположного знаку числа  $a$  (или, яснее, когда обе границы имеют тот же знак, что и  $a$ , или одна из них имеет знак, одинаковый с  $a$ , а другая равна нулю); нижний же — тогда, когда ни одна из границ не имеет того же знака, что  $a$ ; во-вторых,  $(\pm \sqrt{D} + b)/a'$  лежит между  $\gamma/\alpha$  и  $\delta/\beta$  (если ни  $\alpha$ , ни  $\beta$  не равны нулю), где имеет место верхний знак, если ни одна из границ не имеет знака, противоположного знаку  $a'$  (или  $a$ ), и нижний — если ни одна из них не имеет того же знака, что и  $a'$  \*.

**Доказательство.** Мы имеем равенства

$$[1] \quad a\alpha^2 + 2b\alpha\gamma - a'\gamma^2 = A$$

$$[2] \quad a\beta^2 + 2b\beta\gamma - a'\delta^2 = -A'.$$

Из них следует

$$[3] \quad \frac{\alpha}{\gamma} = \frac{\pm \sqrt{D + \frac{aA}{\gamma^2}} - b}{a},$$

$$[4] \quad \frac{\beta}{\delta} = \frac{\pm \sqrt{D - \frac{aA'}{\delta^2}} - b}{a},$$

$$[5] \quad \frac{\gamma}{\alpha} = \frac{\pm \sqrt{D - \frac{a'A}{\alpha^2}} + b}{a'},$$

$$[6] \quad \frac{\delta}{\beta} = \frac{\pm \sqrt{D + \frac{a'A'}{\beta^2}} + b}{a'}.$$

---

\* Очевидно, что других случаев быть не может, так как, согласно предыдущему пункту, вследствие равенства  $\alpha\delta - \beta\gamma = \pm 1$  обе границы не могут иметь противоположных знаков и не могут одновременно быть равны нулю.

Если равно нулю какое-либо из чисел  $\gamma$ ,  $\delta$ ,  $\alpha$ ,  $\beta$ , то отбрасывается соответственно равенство [3], [4], [5], [6]. Однако здесь остается неясным, какими знаками должны быть снабжены величины корней. Это мы установим следующим образом.

Тотчас же ясно, что в [3] и [4] обязательно должны быть взяты верхние знаки, если ни  $\alpha/\gamma$ , ни  $\beta/\delta$  не имеют знаков, противоположных знаку  $a$ , потому что если бы мы взяли нижний знак, то величины  $a\alpha/\gamma$  и  $a\beta/\delta$  были бы отрицательными. Так как, однако,  $A$  и  $A'$  имеют одинаковые знаки,  $\sqrt{D}$  попадает между  $\sqrt{D + aA/\gamma^2}$  и  $\sqrt{D - aA'/\delta^2}$ , и потому в этом случае  $(\sqrt{D} - b)/a$  лежит между  $\alpha/\gamma$  и  $\beta/\delta$ . Тем самым первая часть нашей теоремы для первого случая доказана.

Тем же способом убеждаемся, что в [5] и [6] обязательно должны быть взяты нижние знаки, если ни  $\gamma/\alpha$ , ни  $\delta/\beta$  не имеют того же знака, что  $a'$  или  $a$ , потому что если бы взять верхний знак, то величины  $a'\gamma/\alpha$  и  $a'\delta/\beta$  обязательно стали бы положительными. Отсюда тотчас же следует, что в этом случае  $(-\sqrt{D} + b)/a'$  лежит между  $\gamma/\alpha$  и  $\delta/\beta$ . Поэтому доказана также и вторая часть теоремы для последнего случая. Если бы теперь можно было так же легко показать, что в [3] и [4] нужно брать нижние знаки, если ни одна из величин  $\alpha/\gamma$ ,  $\beta/\delta$  не имеет того же знака, что и  $a$ , и в [5] и [6] — верхние, если ни  $\gamma/\alpha$ , ни  $\delta/\beta$  не имеют знака, противоположного знаку  $a$ , то отсюда подобным же образом следовало бы, что в первом случае  $(-\sqrt{D} - b)/a$  лежит между  $\alpha/\gamma$  и  $\beta/\delta$ , а во втором случае  $(\sqrt{D} + b)/a'$  лежит между  $\gamma/\alpha$  и  $\delta/\beta$ , т. е. первая часть теоремы была бы доказана также и для последнего случая, а вторая часть ее также и для первого случая. Однако, хотя это сделать и нетрудно, все же это не удастся напрямик, и потому мы используем следующий метод.

Если ни одно из чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$  не равно нулю, то  $\alpha/\gamma$  и  $\beta/\delta$  будут иметь те же знаки, что  $\gamma/\alpha$  и  $\delta/\beta$ . Если поэтому ни одна из этих двух величин не имеет того же знака, что  $a'$  или  $a$ , и потому  $(-\sqrt{D} + b)/a'$  попадает между  $\gamma/\alpha$  и  $\delta/\beta$ , то ни одна из величин  $\alpha/\gamma$ ,  $\beta/\delta$  не будет иметь того же знака, что и  $a$ , и потому  $\frac{a'}{-\sqrt{D} + b} =$

$= \frac{-\sqrt{D}-b}{a}$  (вследствие  $aa' = D - b^2$ ) попадет между  $\alpha/\gamma$  и  $\beta/\delta$ . Поэтому для того случая, когда ни  $\alpha$ , ни  $\beta$  не равны нулю, первая часть теоремы доказана также и для второго случая (действительно, то условие, что ни  $\gamma$ , ни  $\delta$  не равны нулю, было добавлено уже в теореме). Аналогичным образом, если ни одно из чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$  не равно нулю, и ни  $\alpha/\gamma$ , ни  $\beta/\delta$  не имеют знака, противоположного знаку  $a$  или  $a'$ , и потому  $(\sqrt{D}-b)/a$  лежит между  $\alpha/\gamma$  и  $\beta/\delta$ , то также и  $\gamma/\alpha$  и  $\delta/\beta$  не будут иметь знака, противоположного знаку  $a'$ , и потому  $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$  попадет между  $\gamma/\alpha$  и  $\delta/\beta$ . Таким образом, если ни  $\gamma$ , ни  $\delta$  не равны нулю, вторая часть теоремы доказана также и для второго случая.

Поэтому остается еще только доказать, что первая часть теоремы справедлива для второго случая и тогда, когда одно из чисел  $\alpha$ ,  $\beta$  равно нулю, и что вторая часть теоремы верна для первого случая также и тогда, когда или  $\gamma = 0$ , или  $\delta = 0$ . Однако все эти случаи невозможны.

Действительно, предположим для первой части теоремы, что ни  $\gamma$ , ни  $\delta$  не равны нулю, что  $\alpha/\gamma$ ,  $\beta/\delta$  не имеют того же знака, что  $a$ .

1. Пусть  $\alpha = 0$ . Тогда из равенства  $\alpha\delta - \beta\gamma = \pm 1$  следует, что  $\beta = \pm 1$ ,  $\gamma = \pm 1$ . Поэтому, вследствие равенства [1],  $A = -a'$  и тем самым  $A$  и  $a'$ , а потому также  $a$  и  $A'$  имеют противоположные знаки, откуда следует, что  $\sqrt{D - aA'/\delta^2} > \sqrt{D} > b$ . Из этого вытекает, что в [4] обязательно должен быть взят нижний знак, потому что иначе  $\beta/\delta$ , очевидно, получило бы тот же знак, что и  $a$ . Поэтому будет  $\frac{\beta}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$  (потому что по определению приведенной формы  $a < \sqrt{D} + b$ ). Это, однако, невозможно, так как  $\beta = \pm 1$  и  $\delta$  не равно нулю.

2. Пусть  $\beta = 0$ . Тогда из равенства  $\alpha\delta - \beta\gamma = \pm 1$  получается, что  $\alpha = \pm 1$ ,  $\delta = \pm 1$ . Поэтому из [2] следует, что  $-A' = -a'$ ; тем самым  $a'$ ,  $a$  и  $A$  будут иметь одинаковые знаки, откуда следует, что  $\sqrt{D + aA/\alpha^2} > \sqrt{D} > b$ . Отсюда вытекает, что в равенстве [3] должен быть взят нижний знак, потому что при ве хнем знаке

$\alpha/\gamma$  получило бы тот же знак, что и  $a$ . Поэтому  $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$ , а это невозможно по той же причине, что и в первом случае (при  $\alpha = 0$ ).

Предположим, для второй части теоремы, что ни  $\alpha$  ни  $\beta$  не равны нулю, что  $\gamma/\alpha$ ,  $\delta/\beta$  не имеют знака, противоположного знаку  $a'$ .

1. Пусть  $\gamma = 0$ . Тогда вследствие равенства  $\alpha\delta - \beta\gamma = \pm 1$  будет  $\alpha = \pm 1$ ,  $\delta = \pm 1$ , и потому из [1] вытекает, что  $A = a$ ; поэтому  $A'$  и  $a'$  будут иметь одинаковые знаки, откуда следует, что  $\sqrt{D + a'A'/\beta^2} > \sqrt{D} > b$ . Поэтому в [6] должен быть взят верхний знак, потому что при нижнем  $\delta/\beta$  получило бы знак, противоположный знаку  $a'$ . Таким образом,  $\delta/\beta > (\sqrt{D} + b)/a' > 1$ . Это, однако, невозможно, так как  $\delta = \pm 1$  и  $\beta$  не равно нулю.

2. Если, наконец,  $\delta = 0$ , то вследствие равенства  $\alpha\delta - \beta\gamma = \pm 1$  будет  $\beta = \pm 1$ ,  $\gamma = \pm 1$  и потому, согласно [2],  $-A' = a$ . Отсюда следует  $\sqrt{D - a'A/\alpha^2} > \sqrt{D} > b$ , в силу чего в [5] надо брать верхний знак. Поэтому  $\frac{\gamma}{\alpha} > \frac{\sqrt{D} + b}{a'} > 1$ , а это невозможно.

Тем самым наша теорема доказана во всей ее полноте.

Так как разность между  $\alpha/\gamma$  и  $\beta/\delta$  равна  $1/\gamma\delta$ , то разность между  $(\pm\sqrt{D}-b)/a$  и  $\alpha/\gamma$  или  $\beta/\delta$  будет меньше чем  $1/\gamma\delta$ ; но между  $(\pm\sqrt{D}-b)/a$  и  $\alpha/\gamma$  или между первой величиной и  $\beta/\delta$  не может лежать дроби, знаменатель которой был бы не больше чем  $\gamma$  или  $\delta$  (предыдущая лемма). Точно также разность между величиной  $(\pm\sqrt{D}+b)/a$  и дробью  $\gamma/\alpha$  или дробью  $\delta/\beta$  будет меньше чем  $1/\alpha\beta$ , и между первой величиной и одной из этих дробей не может лежать дроби, знаменатель которой был бы не больше чем  $\alpha$  и  $\beta$ .

Из применения предшествующей теоремы к алгоритму п. 188 следует, что величина  $(\sqrt{D}-b)/a$ , которую мы обозначим через  $L$ , лежит между  $\alpha'/\gamma'$  и  $\beta'/\delta'$ , между  $\alpha''/\delta''$  и  $\beta''/\delta''$ , между  $\alpha'''/\gamma'''$  и  $\beta'''/\delta'''$  и т. д. (действительно, из п. 189, 3 легко получить, что ни одна из этих границ не имеет знака, противоположного знаку  $a$ , и

потому величина корня  $\sqrt{D}$  должна браться с положительным знаком), или между  $\alpha'/\gamma'$  и  $\alpha''/\gamma''$ , между  $\alpha''/\gamma''$  и  $\alpha'''/\gamma'''$  и т. д. Поэтому все дроби  $\alpha'/\gamma'$ ,  $\alpha'''/\gamma'''$ ,  $\alpha''''/\gamma''''$ , ... будут лежать по одну сторону от  $L$ , а все дроби  $\alpha''/\gamma''$ ,  $\alpha''''/\gamma''''$ ,  $\alpha''''''/\gamma''''''$ , ... — по другую сторону. Так как, однако,  $\gamma' < \gamma'''$ , то  $\alpha'/\gamma'$  лежит вне интервала между  $\alpha'''/\gamma'''$  и  $L$ , и по аналогичной причине  $\alpha''/\gamma''$  — вне интервала между  $L$  и  $\alpha''''/\gamma''''$ ,  $\alpha'''/\gamma'''$  — вне интервала между  $L$  и  $\alpha''''''/\gamma''''''$  и т. д. Отсюда ясно, что эти величины лежат в следующей последовательности:

$$\frac{\alpha'}{\gamma'}, \quad \frac{\alpha'''}{\gamma'''}, \quad \frac{\alpha''''}{\gamma''''}, \dots, L, \dots, \frac{\alpha''''''}{\gamma''''''}, \frac{\alpha''''}{\gamma''''}, \frac{\alpha''}{\gamma''}.$$

Но разность между  $\alpha'/\gamma'$  и  $L$  меньше разности между  $\alpha'/\gamma'$  и  $\alpha''/\gamma''$ , т. е. меньше чем  $1/\gamma'\gamma''$ , и по подобной же причине разность между  $\alpha''/\gamma''$  и  $L$  меньше чем  $1/\gamma''\gamma'''$ , и т. д. Поэтому дроби  $\alpha'/\gamma'$ ,  $\alpha''/\gamma''$ ,  $\alpha'''/\gamma'''$ , ... все больше приближаются к границе  $L$ , и так как  $\gamma'$ ,  $\gamma''$ ,  $\gamma'''$ , ... возрастают до бесконечности, разность между дробями и границей может быть сделана меньше любой заданной величины.

Согласно п. 189, ни одна из величин  $\gamma/\alpha$ ,  $\gamma'/\alpha$ ,  $\gamma''/\alpha$ , ... не имеет того же знака, что  $a$ ; отсюда следует посредством совершенно аналогичного предыдущему ряду заключений, что эти величины и величина  $(-\sqrt{D} + b)/a'$ , которую мы обозначим через  $L'$ , расположены в следующей последовательности:

$$\frac{\gamma}{\alpha}, \quad \frac{\gamma''}{\alpha}, \quad \frac{\gamma'''}{\alpha}, \dots, L', \dots, \frac{\gamma''''}{\alpha}, \frac{\gamma'''}{\alpha}, \frac{\gamma'}{\alpha}.$$

Но разность между  $\gamma/\alpha$  и  $L'$  меньше, чем  $1/\alpha\alpha'$ , разность между  $\gamma'/\alpha$  и  $L'$  меньше чем  $1/\alpha'\alpha''$  и т. д. Поэтому дроби  $\gamma/\alpha$ ,  $\gamma'/\alpha$ , ... все больше приближаются к границе  $L'$ , и разность может быть сделана меньше любой заданной величины.

В примере п. 188  $L = \frac{\sqrt{79} - 8}{3} = 0,2960648$  и приближающие дроби суть  $0/1$ ,  $1/3$ ,  $2/7$ ,  $3/10$ ,  $5/17$ ,  $8/27$ ,  $45/152$ ,  $143/483$ , ... Но  $143/483 = 0,2960662$ . Точно так же  $L' = \frac{-\sqrt{79} + 8}{5} = -0,1776388$ , и приближающие дроби суть  $0/1$ ,  $-1/5$ ,  $-1/6$ ,  $-2/11$ ,  $-3/17$ ,  $-8/45$ ,  $-27/152$ ,  $-143/805$ , ... Но  $143/805 = 0,1776397$ .

**Теорема.** Если приведенные формы  $f, F$  собственно эквивалентны, то одна содержится в периоде другой.

Пусть  $f = (a, b, -a')$ ,  $F = (A, B, -A')$ , определители этих форм равны  $D$ , и первая переходит во вторую при собственной подстановке  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ . Тогда я утверждаю, что если найти период формы  $f$  и бесконечные в обе стороны ряды приведенных форм и преобразований формы  $f$  в них, как это делалось в п. 188, то или  $+\mathfrak{A}$  равно какому-нибудь члену ряда  $\dots, \alpha, \alpha', \alpha, \alpha', \alpha, \dots$ , и если положить его равным  $\alpha^{(m)}$ , то  $+\mathfrak{B} = \beta^{(m)}$ ,  $+\mathfrak{C} = \gamma^{(m)}$ ,  $+\mathfrak{D} = \delta^{(m)}$ , или  $-\mathfrak{A}$  равно одному из членов  $\alpha^{(m)}$  и  $-\mathfrak{B}, -\mathfrak{C}, -\mathfrak{D}$  соответственно равны  $\beta^{(m)}, \gamma^{(m)}, \delta^{(m)}$  (где  $m$  может обозначать также и отрицательный индекс). В обоих случаях  $F$ , очевидно, идентична  $f^{(m)}$ .

**Доказательство.** I. Мы имеем четыре равенства:

$$\begin{aligned} [1] \quad & a\mathfrak{A}^2 + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}^2 = A, \\ [2] \quad & a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B, \\ [3] \quad & a\mathfrak{B}^2 + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}^2 = -A', \\ [4] \quad & \mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1. \end{aligned}$$

Рассмотрим, однако, сначала случай, когда одно из чисел  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$  равно нулю.

1. Если  $\mathfrak{A} = 0$ , то из [4] следует, что  $\mathfrak{B}\mathfrak{C} = -1$ , и потому  $\mathfrak{B} = \pm 1$ ,  $\mathfrak{C} = \mp 1$ . Поэтому из [1] получается  $-a' = A$ , из [2] получается  $-b \pm a'\mathfrak{D} = B$ , или  $B \equiv -b \pmod{a'}$  или  $A$ , откуда следует, что форма  $(A, B, -A')$  является соседней справа для формы  $(a, b, -a')$ . Но так как первая форма приведенная, она обязательно совпадает с  $f'$ . Поэтому  $B = b'$ , и потому, в силу [2],  $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$ ; отсюда, так как  $\frac{b + b'}{-a'} = h'$ , следует, что  $\mathfrak{D} = \mp h'$ . Отсюда же мы заключаем, что  $\mp \mathfrak{A}, \mp \mathfrak{B}, \mp \mathfrak{C}, \mp \mathfrak{D}$  соответственно равны  $0, -1, +1, h'$ , т. е. равны  $\alpha', \beta', \gamma', \delta'$ .

2. Если  $\mathfrak{B} = 0$ , то из [4] следует, что  $\mathfrak{A} = \pm 1$ ;  $\mathfrak{D} = \pm 1$ ; из [3] — что  $a' = A'$ , из [2] — что  $b \mp a'\mathfrak{C} = B$ , или  $b \equiv B \pmod{a'}$ . Так как, однако, как  $f$ , так и  $F$  — приведенные формы, то как  $b$ , так и  $B$  будут лежать между  $\sqrt{D}$  и  $\sqrt{D} \mp a'$  (в зависимости от того,

положительно  $a'$  или отрицательно; п. 184, 5). Поэтому обязательно  $b = B$  и  $\mathfrak{C} = 0$ . Следовательно, формы  $f$  и  $F$  совпадают, и  $\pm \mathfrak{A}$ ,  $\pm \mathfrak{B}$ ,  $\pm \mathfrak{C}$ ,  $\pm \mathfrak{D}$  соответственно равны 1, 0, 0, 1, т. е. равны  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$ .

3. Если  $\mathfrak{C} = 0$ , то из [4] следует, что  $\mathfrak{A} = \pm 1$ ,  $\mathfrak{D} = \pm 1$ , из [1] — что  $a = A$ , из [2] — что  $\pm a\mathfrak{B} + b = B$ , или  $b \equiv B \pmod{a}$ . Так как, однако, как  $b$ , так и  $B$  лежат между  $\sqrt{D}$  и  $\sqrt{D} \mp a$ , то обязательно будет  $B = b$  и  $\mathfrak{B} = 0$ . Поэтому этот случай не отличается от предыдущего.

4. Если  $\mathfrak{D} = 0$ , то из [4] следует, что  $\mathfrak{B} = \pm 1$ ,  $\mathfrak{C} = \mp 1$ , из [3] — что  $a = -A'$ , из [2] — что  $\pm a\mathfrak{A} - b = B$ , или  $B \equiv -b \pmod{a}$ . Поэтому  $F$  является соседней слева для формы  $f$ , и, значит, совпадает с формой  $'f$ . Поэтому, вследствие  $\frac{'b + b}{a} = h$  и  $B = 'b$ , будет  $\pm \mathfrak{A} = h$ . Отсюда следует, что  $\pm \mathfrak{A}$ ,  $\pm \mathfrak{B}$ ,  $\pm \mathfrak{C}$ ,  $\pm \mathfrak{D}$  соответственно равны  $h$ , 1,  $-1$ , 0, т. е.  $'\alpha$ ,  $'\beta$ ,  $'\gamma$ ,  $'\delta$ .

Итак, остается только тот случай, когда ни одно из чисел  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$ ,  $\mathfrak{D}$  не равно нулю. Здесь, вследствие леммы п. 190, величины  $\mathfrak{A}/\mathfrak{C}$ ,  $\mathfrak{B}/\mathfrak{D}$ ,  $\mathfrak{C}/\mathfrak{A}$ ,  $\mathfrak{D}/\mathfrak{B}$  будут иметь одинаковые знаки, и потому могут представиться два случая, так как эти знаки могут или совпадать со знаком  $a$ ,  $a'$ , или быть ему противоположными.

II. Если  $\mathfrak{A}/\mathfrak{C}$ ,  $\mathfrak{B}/\mathfrak{D}$  имеют тот же знак, что и  $a$ , то величина  $(\sqrt{D - b})/a$  (которую мы обозначим через  $L$ ) будет лежать между этими дробями (п. 191). Теперь мы покажем, что  $\mathfrak{A}/\mathfrak{C}$  равно одной из дробей  $\alpha''/\gamma''$ ,  $\alpha'''/\gamma'''$ ,  $\alpha''''/\gamma''''$ , ..., и  $\mathfrak{B}/\mathfrak{D}$  равно следующей, или, что если  $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^{(m)}}{\gamma^{(m)}}$ , то  $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{(m+1)}}{\gamma^{(m+1)}}$ . В предыдущем пункте

мы показали, что величины  $\alpha'/\gamma'$ ,  $\alpha''/\gamma''$ ,  $\alpha'''/\gamma'''$ , ... (которые мы коротко обозначим через (1), (2), (3), ...) располагаются в следующей последовательности (I): (1), (3), (5), ...,  $L$ , ..., (6), (4), (2); первая из этих величин равна нулю (так как  $\alpha' = 0$ ), остальные имеют те же самые знаки, что  $L$  или  $a$ . Так как, однако, по предположению,  $\mathfrak{A}/\mathfrak{C}$ ,  $\mathfrak{B}/\mathfrak{D}$  (вместо которых мы будем писать  $\mathfrak{M}$ ,  $\mathfrak{N}$ ) имеют одинаковые знаки, то эти величины, очевидно, будут лежать справа от (1) (или, если угодно, с той же стороны, что и  $L$ ), и притом, так как  $L$  лежит между ними, одни справа от  $L$ , а

другая слева от  $L$ . Но легко можно показать, что  $\mathfrak{M}$  не может лежать справа от (2), так как иначе  $\mathfrak{N}$  лежало бы между (1) и  $L$ , откуда следовало бы, во-первых, что (2) лежит между  $\mathfrak{M}$  и  $\mathfrak{N}$ , и потому знаменатель дроби (2) больше, чем знаменатель дроби  $\mathfrak{N}$  (п. 190), и во-вторых, что  $\mathfrak{N}$  лежит между (1) и (2), и потому знаменатель дроби  $\mathfrak{N}$  больше, чем знаменатель дроби (2), что невозможно.

Мы предположим, что  $\mathfrak{M}$  не равно ни одной из дробей (2), (3), (4), ... и посмотрим, что из этого следует. Очевидно, что если дробь  $\mathfrak{M}$  лежит левее, чем  $L$ , она обязательно должна лежать или между (1) и (3), или между (3) и (5), или между (5) и (7) и т. д. (так как  $L$  иррационально и потому, очевидно, отлично от  $\mathfrak{M}$ , а дроби (1), (3), (5), ... могут быть приближены к  $L$  на любую заданную величину). Если же  $\mathfrak{M}$  лежит справа от  $L$ , то оно должно обязательно лежать или между (2) и (4), или между (4) и (6), или между (6) и (8) и т. д. Поэтому, если мы предположим, что  $\mathfrak{M}$  лежит между  $(m)$  и  $(m+2)$ , то величины  $\mathfrak{M}$ ,  $(m)$ ,  $(m+1)$ ,  $(m+2)$ ,  $L$ , очевидно, будут лежать в следующей последовательности:

$$(II) \quad * \quad (m), \mathfrak{M}, (m+2), L, (m+1).$$

Тогда обязательно  $\mathfrak{N} = (m+1)$ . Действительно,  $\mathfrak{N}$  лежит справа от  $L$ ; если бы оно лежало также и справа от  $(m+1)$ , то  $(m+1)$  лежало бы между  $\mathfrak{M}$  и  $\mathfrak{N}$ , т. е. было бы  $\gamma^{(m+1)} > \mathfrak{E}$ , а  $\mathfrak{M}$  лежало бы между  $(m)$  и  $(m+1)$ , т. е. было бы  $\mathfrak{E} > \gamma^{(m+1)}$  (п. 190), что невозможно. А если бы  $\mathfrak{N}$  лежало слева от  $(m+1)$ , т. е. между  $(m+2)$  и  $(m+1)$ , то было бы  $\mathfrak{D} > \gamma^{(m+2)}$ , и так как  $(m+2)$  лежит между  $\mathfrak{M}$  и  $\mathfrak{N}$ , было бы  $\gamma^{(m+2)} > \mathfrak{D}$ , что невозможно. Поэтому  $\mathfrak{N} = (m+1)$ ,

$$\text{или} \quad \frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{(m+1)}}{\gamma^{(m+1)}} = \frac{\beta^{(m)}}{\delta^{(m)}}.$$

Так как  $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{E} = 1$ , то  $\mathfrak{B}$  взаимно просто с  $\mathfrak{D}$ , и по подобной же причине  $\beta^{(m)}$  взаимно просто с  $\delta^{(m)}$ . Отсюда легко видеть,

---

\* Безразлично, совпадает ли порядок расположения в (II) с порядком расположения в (I) или является ему противоположным, т. е. лежит ли в (I) величина  $(m)$  слева или справа от  $L$ .



что равенство  $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\beta^{(m)}}{\delta^{(m)}}$  может выполняться только в том случае, если или  $\mathfrak{B} = \beta^{(m)}$ ,  $\mathfrak{D} = \delta^{(m)}$ , или  $\mathfrak{B} = -\beta^{(m)}$ ,  $\mathfrak{D} = -\delta^{(m)}$ .

Но так как форма  $f$  при собственной подстановке  $\alpha^{(m)}$ ,  $\beta^{(m)}$ ,  $\gamma^{(m)}$ ,  $\delta^{(m)}$  переходит в форму  $f^{(m)}$ , которая есть  $(\pm a^{(m)}, b^{(m)}, \pm a^{(m+1)})$ , то мы имеем равенства

$$[5] \quad a\alpha^{(m)^2} + 2b\alpha^{(m)}\gamma^{(m)} - a'\gamma^{(m)^2} = \pm a^{(m)},$$

$$[6] \quad a\alpha^{(m)}\beta^{(m)} + b(\alpha^{(m)}\delta^{(m)} + \beta^{(m)}\gamma^{(m)}) - a'\gamma^{(m)}\delta^{(m)} = b^{(m)},$$

$$[7] \quad a\beta^{(m)^2} + 2b\beta^{(m)}\delta^{(m)} - a'\delta^{(m)^2} = \mp a^{(m+1)},$$

$$[8] \quad \alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)} = 1.$$

Поэтому (из равенств [7] и [3]) получается  $\mp a^{(m+1)} = -A'$ . Если, далее, умножить равенство [2] на  $\alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)}$ , равенство [6] на  $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C}$  и вычесть, то, раскрывая скобки, легко установить равенство

$$[9] \quad B - b^{(m)} = (\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)})[a\mathfrak{B}\beta^{(m)} + b(\mathfrak{D}\beta^{(m)} + \mathfrak{B}\delta^{(m)}) - a'\mathfrak{D}\delta^{(m)}] + \\ + (\mathfrak{B}\delta^{(m)} - \mathfrak{D}\beta^{(m)})[a\mathfrak{A}\alpha^{(m)} + b(\mathfrak{C}\alpha^{(m)} + \mathfrak{A}\gamma^{(m)}) - a'\mathfrak{C}\gamma^{(m)}],$$

и так как либо  $\beta^{(m)} = \mathfrak{B}$ ,  $\delta^{(m)} = \mathfrak{D}$ , либо  $\beta^{(m)} = -\mathfrak{B}$ ,  $\delta^{(m)} = -\mathfrak{D}$ , то отсюда следует, что  $B - b^{(m)} = \pm (\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)})(a\mathfrak{B}^2 + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}^2) = \mp (\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)})A'$ .

Поэтому  $B \equiv b^{(m)} \pmod{A'}$ . Так как, однако, как  $B$ , так и  $b^{(m)}$  лежат между  $\sqrt{D}$  и  $\sqrt{D} \mp A$ , то обязательно  $B = b^{(m)}$ , и потому  $\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)} = 0$ , или  $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^{(m)}}{\gamma^{(m)}}$ , т. е.  $\mathfrak{M} = (m)$ .

Таким образом, из предположения, что  $\mathfrak{M}$  не равно ни одной из величин (2), (3), (4), ..., мы вывели, что в действительности оно равно одной из них. Если же мы теперь с самого начала предположим, что  $\mathfrak{M} = (m)$ , то, очевидно, будет или  $\mathfrak{A} = \alpha^{(m)}$  и  $\mathfrak{C} = \gamma^{(m)}$ , или  $-\mathfrak{A} = \alpha^{(m)}$ ,  $-\mathfrak{C} = \gamma^{(m)}$ . В обоих случаях из [1] и [5] следует, что  $A = \pm a^{(m)}$ , и из [9] — что  $B - b^{(m)} = \pm (\mathfrak{B}\delta^{(m)} - \mathfrak{D}\beta^{(m)})A$ , или  $B \equiv b^{(m)} \pmod{A}$ . Отсюда, аналогично тому, как и выше, получается  $B = b^{(m)}$ , и потому  $\mathfrak{B}\delta^{(m)} = \mathfrak{D}\beta^{(m)}$ ; но так как  $\mathfrak{B}$  взаимно просто с  $\mathfrak{D}$ , и  $\beta^{(m)}$  взаимно просто с  $\delta^{(m)}$ , то, следовательно, или  $\mathfrak{B} = \beta^{(m)}$ ,  $\mathfrak{D} = \delta^{(m)}$ , или  $\mathfrak{B} = -\beta^{(m)}$ ,  $\mathfrak{D} = -\delta^{(m)}$ , и тем самым

из [7] следует, что  $-A' = \mp a^{(m+1)}$ . Поэтому формы  $F$  и  $f^{(m)}$  совпадают. Но при помощи равенства  $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)}$  без труда доказывается, что  $+\mathfrak{B} = \beta^{(m)}$ ,  $+\mathfrak{D} = \delta^{(m)}$ , если  $+\mathfrak{A} = \alpha^{(m)}$ ,  $+\mathfrak{C} = \gamma^{(m)}$ , и, наоборот, нужно положить  $-\mathfrak{B} = \beta^{(m)}$ ,  $-\mathfrak{D} = \delta^{(m)}$ , если  $-\mathfrak{A} = \alpha^{(m)}$ ,  $-\mathfrak{C} = \gamma^{(m)}$ . Это и нужно было доказать.

III. Если знак величин  $\mathfrak{A}/\mathfrak{C}$ ,  $\mathfrak{B}/\mathfrak{D}$  противоположен знаку  $a$ , то доказательство настолько похоже на предыдущее, что достаточно указать только на основные пункты. Число  $(-\sqrt{D} + b)/a'$  лежит между  $\mathfrak{C}/\mathfrak{A}$  и  $\mathfrak{D}/\mathfrak{B}$ . Дробь  $\mathfrak{D}/\mathfrak{B}$  равна какой-нибудь из дробей

$$(I) \quad \frac{{}'\delta}{{}'\beta}, \quad \frac{''\delta}{''\beta}, \quad \frac{'''\delta}{'''\beta}, \quad \dots,$$

и если считать ее равной  ${}^{(m)}\delta/{}^{(m)}\beta$ , то

$$(II) \quad \frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{(m)}\gamma}{{}^{(m)}\alpha}.$$

(I) доказывается следующим образом. Если предположить, что  $\mathfrak{D}/\mathfrak{B}$  не равно ни одной из этих дробей, то она должна лежать между какими-нибудь двумя из них:  ${}^{(m)}\delta/{}^{(m)}\beta$  и  ${}^{(m+2)}\delta/{}^{(m+2)}\beta$ . А отсюда тем же способом, что и выше, можно вывести, что обязательно

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{(m+1)}\delta}{{}^{(m+1)}\beta} = \frac{{}^{(m)}\gamma}{{}^{(m)}\alpha},$$

и потому или  $\mathfrak{A} = {}^{(m)}\alpha$ ,  $\mathfrak{C} = {}^{(m)}\gamma$ , или  $-\mathfrak{A} = {}^{(m)}\alpha$ ,  $-\mathfrak{C} = {}^{(m)}\gamma$ . Так как, однако,  $f$  при собственной подстановке  ${}^{(m)}\alpha$ ,  ${}^{(m)}\beta$ ,  ${}^{(m)}\gamma$ ,  ${}^{(m)}\delta$  переходит в форму

$${}^{(m)}f = (\pm {}^{(m)}a, {}^{(m)}b, \mp {}^{(m-1)}a),$$

то получаются три равенства, из которых в связи с равенствами [1] [2], [3], [4] и равенством  ${}^{(m)}\alpha {}^{(m)}\delta = {}^{(m)}\beta {}^{(m)}\gamma = 1$  подобным же образом, как выше, вытекает, что первый член  $A$  формы  $F$  равен первому члену формы  ${}^{(m)}f$ , и средний член [первой сравним со средним членом второй по модулю  $A$ . Отсюда, так как обе формы

приведенные и потому средние члены обеих лежат между  $V\bar{D}$  и  $V\bar{D} \mp A$ , следует, что эти средние члены равны, а отсюда выводится, что  $\frac{{}^{(m)}\delta}{{}^{(m)}\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$ . Поэтому здесь справедливость утверждения (I) выведена из предположения, что оно не верно.

Если же предположить, что  $\frac{{}^{(m)}\delta}{{}^{(m)}\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$ , то совершенно аналогичным образом и при помощи тех же равенств доказывается и (II), т. е. что  $\frac{{}^{(m)}\gamma}{{}^{(m)}\alpha} = \frac{\mathfrak{C}}{\mathfrak{A}}$ . А отсюда вследствие равенств  $\mathfrak{A}\mathfrak{D} = \mathfrak{B}\mathfrak{C} = 1$ ,  ${}^{(m)}\alpha{}^{(m)}\delta = {}^{(m)}\beta{}^{(m)}\gamma = 1$  вытекает, что или

$$\mathfrak{A} = {}^{(m)}\alpha, \quad \mathfrak{B} = {}^{(m)}\beta, \quad \mathfrak{C} = {}^{(m)}\gamma, \quad \mathfrak{D} = {}^{(m)}\delta.$$

или

$$-\mathfrak{A} = {}^{(m)}\alpha, \quad -\mathfrak{B} = {}^{(m)}\beta, \quad -\mathfrak{C} = {}^{(m)}\gamma, \quad -\mathfrak{D} = {}^{(m)}\delta,$$

и что формы  $F$  и  ${}^{(m)}f$  совпадают, а это и требовалось доказать.

## 194

Так как формы, которые выше (п. 187, 6) мы называли ассоциированными формами, всегда несобственно эквивалентны (п. 159), то ясно, что если приведенные формы  $F, f$  несобственно эквивалентны, и  $G$  есть форма, ассоциированная с  $F$ , то формы  $G, f$  собственно эквивалентны, и потому форма  $G$  содержится в периоде формы  $f$ . Если поэтому формы  $F$  и  $f$  эквивалентны как собственно, так и несобственно, то как  $F$ , так и  $G$  будут, очевидно, содержаться в периоде формы  $f$ . Поэтому этот период будет ассоциирован с самим собой и будет содержать две двусторонние формы (п. 187, 7). Тем самым мы получаем красивое подтверждение теоремы из п. 165, на основании которого мы уже могли бы быть уверенными, что существует хотя бы одна двусторонняя форма, которая эквивалентна формам  $F, f$ .

**Задача.** Пусть даны какие-нибудь две формы  $\Phi$  и  $\varphi$  с одинаковым определителем; требуется узнать, эквивалентны они или нет.

**Решение.** Найдем две приведенные формы  $F$  и  $f$ , которые соответственно эквивалентны заданным формам  $\Phi$  и  $\varphi$  (п. 183). В зависимости от того, эквивалентны ли эти формы только собственно, или только несобственно, или и собственно и несобственно, или ни так, ни иначе, также и заданные формы будут эквивалентны или только собственно, или только несобственно, или и так и иначе, или ни так, ни иначе. Найдем период одной из этих приведенных форм, например, период формы  $f$ . Если в этот период входит форма  $F$ , но одновременно не входит форма, ассоциированная с  $F$ , то, очевидно, имеет место *первый* случай. Если же входит эта ассоциированная форма, а сама  $F$  не входит, то *второй*, если обе формы входят — то *третий*, а если не входит ни одна из них, то *четвертый* случай.

**Пример.** Пусть заданы формы  $(129, 92, 65)$ ,  $(42, 59, 81)$  с определителем 79. В качестве эквивалентных им приведенных форм находим  $(10, 7, -3)$ ,  $(5, 8, -3)$ . Период первой формы следующий:

$(10, 7, -3)$ ,  $(-3, 8, 5)$ ,  $(5, 7, -6)$ ,  $(-6, 5, 9)$ ,  $(9, 4, -7)$ ,  $(-7, 3, 10)$ .

Так как в нем нет формы  $(5, 8, -3)$ , но есть ассоциированная с ней форма  $(-3, 8, 5)$ , то заданные формы эквивалентны только несобственно.

Если все приведенные формы с одинаковым определителем разбиты на периоды  $P, Q, R, \dots$  тем способом, который был указан выше (п. 187, 5), и из каждого периода выбрана по желанию любая форма, например, из  $P$  выбрана  $F$ , из  $Q$  выбрана  $G$ , из  $R$  выбрана  $H$  и т. д., то среди этих форм  $F, G, H, \dots$  не может быть никаких двух, которые собственно эквивалентны. А каждая другая форма с тем же определителем будет эквивалентна какой-нибудь из них, причем только одной. Из этого вытекает, что все формы с этим определителем могут быть разбиты на столько классов, сколько имеется периодов, именно, если отнести к первому классу те, которые собственно эквивалентны форме  $F$ , ко второму — те, которые собственно эквивалентны форме  $G$  и т. д. Таким образом, все формы, содержащиеся в одном и том же классе, будут собственно эквивалентны; формы же из раз-

личных классов не могут быть собственно эквивалентными. Однако здесь мы не будем задерживаться на этом вопросе, который должен быть подробнее рассмотрен ниже.

## 196

**Задача.** Пусть даны две собственно эквивалентные формы  $\Phi$  и  $\varphi$ ; требуется найти собственное преобразование одной из них в другую.

**Решение.** Методом п. 183 можно найти два ряда форм

$$\Phi, \Phi', \Phi'', \dots, \Phi^{(n)} \quad \text{и} \quad \varphi, \varphi', \varphi'', \dots, \varphi^{(\nu)}$$

с тем свойством, что каждая следующая форма собственно эквивалентна предыдущей, а последние формы  $\Phi^{(n)}$  и  $\varphi^{(\nu)}$  — приведенные; и так как мы предположили, что  $\Phi$  и  $\varphi$  собственно эквивалентны, то обязательно  $\Phi^{(n)}$  встретится в периоде формы  $\varphi^{(\nu)}$ . Пусть  $\varphi^{(\nu)} = f$  и период ее до формы  $\Phi^{(n)}$  следующий:

$$f, f', f'', \dots, f^{(m-1)}, \Phi^{(n)},$$

так что в этом периоде индекс формы  $\Phi^{(n)}$  равен  $m$ ; обозначим еще те формы, которые противоположны формам, ассоциированным с  $\Phi, \Phi', \Phi'', \dots, \Phi^{(n)}$  соответственно через

$$\Psi, \Psi', \Psi'', \dots, \Psi^{(n)} *.$$

Тогда в ряду  $\varphi, \varphi', \varphi'', \dots, f, f', f'', \dots, f^{(m-1)}, \Psi^{(n-1)}, \Psi^{(n-2)}, \dots, \Psi, \Phi$  каждая форма будет соседней слева для предыдущей, и потому, согласно п. 177, может быть найдено собственное преобразование первой формы,  $\varphi$ , в последнюю,  $\Phi$ . Для всех остальных форм, кроме  $f^{(m-1)}$  и  $\Psi^{(n-1)}$ , это непосредственно очевидно. Для этой же пары форм доказательство следующее. Пусть  $f^{(m-1)} = (g, h, i)$ ,  $f^{(m)} = \Phi^{(n)} = (g', h', i')$ ,  $\Phi^{(n-1)} = (g'', h'', i'')$ . Форма  $(g', h', i')$  будет соседней справа как для формы  $(g, h, i)$ , так и для  $(g'', h'', i'')$ , поэтому  $i = g' = i''$  и  $-h \equiv h' \equiv -h'' \pmod{i}$  или  $g$ , или  $i''$ .

---

\* Таким образом,  $\Psi$  получается из  $\Phi$  перестановкой первого и последнего членов и изменением знака у среднего члена; аналогично обстоит дело и для других форм.

Отсюда вытекает, что форма  $(i'', -h'', g'')$ , т. е. форма  $\Psi^{(n-1)}$  — соседняя справа для формы  $(g, h, i)$ , т. е. формы  $f^{(m-1)}$ .

Если формы  $\Phi, \varphi$  несобственно эквивалентны, то форма  $\varphi$  будет собственно эквивалентна той форме, которая противоположна  $\Phi$ . Поэтому можно найти собственное преобразование формы  $\varphi$  в ту форму, которая противоположна  $\Phi$ . Если предположить, что это достигается подстановкой  $\alpha, \beta, \gamma, \delta$ , то легко видеть, что  $\varphi$  несобственно преобразуется в самую форму  $\Phi$  подстановкой  $\alpha, -\beta, \gamma, -\delta$ .

Отсюда также очевидно, что если формы  $\Phi$  и  $\varphi$  эквивалентны как собственно, так и несобственно, то могут быть найдены два преобразования, одно собственное и одно несобственное.

**Пример.** Найдем несобственное преобразование формы (129, 92, 65) в форму (42, 59, 81), которая, как мы установили в предыдущем пункте, несобственно эквивалентна первой. Сначала надо найти собственное преобразование формы (129, 92, 65) в форму (42, —59, 81). Для этого строим следующий ряд форм: (129, 92, 65), (65, —27, 10), (10, 7, —3), (—3, 8, 5), (5, 22, 81), (81, 59, 42), (42, —59, 81). Отсюда находим собственное преобразование —47, 56, 73, —87, при котором (129, 92, 65) переходит в (42, —59, 81). Поэтому первая форма будет переходить в форму (42, 59, 81) при несобственном преобразовании —47, —56, 73, 87.

Если имеется *одно* преобразование какой-нибудь формы  $\varphi = (a, b, c)$  в эквивалентную форму  $\Phi$ , то из него можно вывести все однотипные преобразования формы  $\varphi$  в  $\Phi$ , если только можно указать *все решения неопределенного уравнения*  $t^2 - Du^2 = m^2$ , в котором  $D$  обозначает определитель форм  $\Phi, \varphi$ , и  $m$  — наибольший общий делитель чисел  $a, 2b, c$  (п. 162). За эту проблему, которая в случае отрицательного значения  $D$  уже была решена выше, мы сейчас возьмемся также и для положительного значения  $D$ . Так как, однако, каждое значение  $t$ , удовлетворяющее уравнению, будет удовлетворять ему и после изменения своего знака, и то же самое верно для значений  $u$ , то нам нужно будет определить лишь все

положительные значения  $t, u$ , и каждое решение с положительными значениями будет заменять четыре решения. Эту задачу мы решим так, что сначала найдем наименьшие значения  $t, u$  (кроме само собой разумеющихся  $t = m, u = 0$ ), а затем научимся выводить из них все остальные.

## 198

**Задача.** Найти наименьшие значения  $t, u$ , удовлетворяющие неопределенному уравнению  $t^2 - Du^2 = m^2$ , если дана форма  $(M, N, P)$ , определитель которой равен  $D$ , и у которой наибольший общий делитель чисел  $M, 2N, P$  равен  $m$ .

**Решение.** Возьмем любую приведенную форму  $f = (a, b, -a')$  с определителем  $D$ , у которой наибольший общий делитель чисел  $a, 2b, a'$  равен  $m$ . То, что такая форма существует, ясно уже из того, что можно найти эквивалентную форме  $(M, N, P)$  приведенную форму, которая, согласно п. 161, обладает этим свойством; однако для нашей цели можно использовать каждую приведенную форму, для которой это условие выполняется. Найдем период формы  $f$ , который пусть состоит из  $n$  форм. При сохранении всех обозначений, которыми мы пользовались в п. 188, имеет место  $f^{(n)} = (a^{(n)}, b^{(n)}, -a^{(n+1)})$ , потому что  $n$  четно, и  $f$  будет переходить в эту форму при собственной подстановке  $\alpha^{(n)}, \beta^{(n)}, \gamma^{(n)}, \delta^{(n)}$ . Но так как  $f$  и  $f^{(n)}$  совпадают, то  $f$  будет переходить в  $f^{(n)}$  и при собственной подстановке  $1, 0, 0, 1$ . Из этих двух однотипных преобразований формы  $f$  в  $f^{(n)}$ , согласно п. 162, может быть выведено решение уравнения  $t^2 - Du^2 = m^2$  в целых числах, именно,  $t = (\alpha^{(n)} + \delta^{(n)})m/2$  (равенство 18 в п. 162),  $u = \gamma^{(n)}m/a$  (равенство 19 в п. 162)\*. Если эти значения, взятые положительными (ибо первоначально они еще не обязаны быть таковыми), обозначить через  $T, U$ , то  $T, U$  будут наименьшими значениями  $t, u$ , кроме  $t = m, u = 0$  (от этих последних  $T$  и  $U$  обязательно отличны, так как  $\gamma^{(n)}$ , очевидно, не может быть равно нулю).

\* То, что в п. 162 обозначалось через  $\alpha, \beta, \gamma, \delta; \alpha', \beta', \gamma', \delta'; A, B, C; a, b, c; e$ , здесь соответственно равно  $1, 0, 0, 1; \alpha^{(n)}, \beta^{(n)}, \gamma^{(n)}, \delta^{(n)}; a, b, -a'; a, b, -a'; 1$ .

Действительно, если мы предположим, что существуют еще меньшие значения  $t$ ,  $u$ , например,  $\mathfrak{t}$  и  $\mathfrak{u}$ , которые положительны, и  $\mathfrak{u}$  не равно нулю, то, согласно п. 162, форма  $f$  при собственной подстановке  $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ ,  $\frac{1}{m}a'\mathfrak{u}$ ,  $\frac{1}{m}a\mathfrak{u}$ ,  $\frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$  будет переходить в идентичную ей форму. Теперь, из п. 193, II следует, что или  $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ , или  $-\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$  должно быть равно одному из чисел  $\alpha''$ ,  $\alpha'''$ ,  $\alpha''''$ , ..., например,  $\alpha^{(\mu)}$  (именно, так как  $t^2 = D\mathfrak{u}^2 + m^2 = b^2\mathfrak{u}^2 + aa'\mathfrak{u}^2 + m^2$ , то  $t^2 > b^2\mathfrak{u}^2$ , и потому  $\mathfrak{t} - b\mathfrak{u}$  положительно; поэтому дробь  $(\mathfrak{t} - b\mathfrak{u})/a\mathfrak{u}$ , которая соответствует дроби  $\mathfrak{A}/\mathfrak{E}$  в п. 193, будет иметь тот же самый знак, что и  $a$  или  $a'$ ), и что в первом случае  $\frac{1}{m}a'\mathfrak{u}$ ,  $\frac{1}{m}a\mathfrak{u}$ ,  $\frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$ , а во втором — эти же величины с противоположными знаками соответственно равны  $\beta^{(\mu)}$ ,  $\gamma^{(\mu)}$ ,  $\delta^{(\mu)}$ . Так как, однако,  $\mathfrak{u} < U$ , т. е.  $\mathfrak{u} < \frac{\gamma^{(n)}m}{a}$  и  $> 0$ , то  $\gamma^{(\mu)}$  будет  $< \gamma^{(n)}$  и  $> 0$ ; поэтому, так как ряд  $\gamma$ ,  $\gamma'$ ,  $\gamma''$ , ... непрерывно возрастает,  $\mu$  обязательно будет лежать между 0 и  $n$ . Но соответствующая форма  $f^{(\mu)}$  будет совпадать, с формой  $f$ . Это, однако, невозможно, так как все формы  $f$ ,  $f'$ ,  $f''$ , ... до  $f^{(n-1)}$  предполагаются различными. Отсюда следует, что  $T$ ,  $U$  являются наименьшими значениями  $t$ ,  $u$  (за исключением  $m$ , 0).

**Пример.** Если  $D = 79$ ,  $m = 1$ , то можно использовать форму (3. 8, —5), для которой  $n = 6$ , и  $\alpha^{(n)} = -8$ ,  $\gamma^{(n)} = -27$ ,  $\delta^{(n)} = -152$  (п. 188). Отсюда следует  $T = 80$ ,  $U = 9$ , что дает наименьшие удовлетворяющие уравнению  $t^2 - 79u^2 = 1$  значения  $t$ ,  $u$ .

Для практического использования могут быть получены еще более удобные формулы. Именно,  $2b\gamma^{(n)} = -a(\alpha^{(n)} - \delta^{(n)})$ , что легко следует из п. 162, если умножить равенство [19] на  $2b$ , равенство [20] — на  $a$  и заменить использованные там обозначения теперешними. Отсюда  $\alpha^{(n)} + \delta^{(n)} = 2\delta^{(n)} - \frac{2b}{a}\gamma^{(n)}$ , и потому

$$\pm T = m \left( \delta^{(n)} - \frac{b}{a} \gamma^{(n)} \right), \quad \pm U = \frac{\gamma^{(n)}m}{a}.$$



Подобным же образом получаются следующие значения:

$$\pm T = m \left( \alpha^{(n)} + \frac{b}{a'} \beta^{(n)} \right), \quad \pm U = \frac{\beta^{(n)} m}{a'}$$

Как первые, так и вторые формулы будут очень удобными, так как  $\gamma^{(n)} = \delta^{(n-1)}$ ,  $\alpha^{(n)} = \beta^{(n-1)}$ , и потому, если пользоваться вторыми формулами, то нужно вычитать только ряд  $\beta', \beta'', \beta''', \dots, \beta^{(n)}$ , а если первыми — то только ряд  $\delta', \delta'', \delta''', \dots$ . Кроме того, из п. 189, 3 легко следует, так как  $n$  обязательно четно, что  $\alpha^{(n)}$  и  $\frac{b}{a'} \beta^{(n)}$  имеют одинаковые знаки, и точно так же  $\delta^{(n)}$  и  $\frac{b}{a} \gamma^{(n)}$ , так что в первых формулах надо брать абсолютную разность, а во вторых — абсолютную сумму, и потому знаки вообще не нужно принимать во внимание. При возвращении к обозначениям, употреблявшимся в п. 189, 4, из первых формул получается

$$T = m [k', k'', k''', \dots, k^{(n)}] - \frac{mb}{a} [k', k'', k''', \dots, k^{(n-1)}],$$

$$U = \frac{m}{a} [k', k'', k''', \dots, k^{(n-1)}]$$

а из вторых

$$T = m [k'', k''', \dots, k^{(n-1)}] + \frac{mb}{a'} [k'', k''', \dots, k^{(n)}],$$

$$U = \frac{m}{a'} [k'', k''', \dots, k^{(n)}],$$

где для значения  $T$  может быть написано также  $m \left[ k'', k''', \dots, k^{(n)} \frac{b}{a'} \right]$ .

**Пример.** Для  $D = 61$ ,  $m = 2$  можно использовать форму (2, 7, —6), для которой находим, что  $n = 6$ , а  $k', k'', k''', k'''', k''''', k''''''$  соответственно равны 2, 2, 7, 2, 2, 7. Отсюда следует

$T = 2 [2, 2, 7, 2, 2, 7] - 7 [2, 2, 7, 2, 2] = 2888 - 1365 = 1523$  по первой формуле; то же значение получается и по второй формуле:

$$T = 2 [2, 7, 2, 2] + \frac{7}{3} [2, 7, 2, 2, 7]$$

и

$$U = [2, 2, 7, 2, 2] = \frac{1}{3} [2, 7, 2, 2, 7] = 195.$$

Впрочем, имеются еще различные приемы, при помощи которых вычисления могут быть сокращены; однако требования краткости не позволяют нам говорить о них подробнее.

200

Чтобы из наименьших значений  $t$ , и получить все, представим уравнение  $T^2 - DU^2 = m^2$  так:

$$\left(\frac{T}{m} + \frac{U}{m} \sqrt{D}\right) \left(\frac{T}{m} - \frac{U}{m} \sqrt{D}\right) = 1,$$

откуда следует, что если  $e$  обозначает любое число, то

$$[1] \quad \left(\frac{T}{m} + \frac{U}{m} \sqrt{D}\right)^e \cdot \left(\frac{T}{m} - \frac{U}{m} \sqrt{D}\right)^e = 1.$$

Теперь ради краткости мы обозначим вообще значения величин

$$\frac{m}{2} \left(\frac{T}{m} + \frac{U}{m} \sqrt{D}\right)^e + \frac{m}{2} \left(\frac{T}{m} - \frac{U}{m} \sqrt{D}\right)^e,$$

$$\frac{m}{2\sqrt{D}} \left(\frac{T}{m} + \frac{U}{m} \sqrt{D}\right)^e - \frac{m}{2\sqrt{D}} \left(\frac{T}{m} - \frac{U}{m} \sqrt{D}\right)^e$$

через  $t^{(e)}$ ,  $u^{(e)}$ , т. е. значения их для  $e = 0$  — через  $t^0$ ,  $u^0$  (которые будут равны  $m$ ,  $0$ ), для  $e = 1$  — через  $t'$ ,  $u'$  (которые будут равны  $T$ ,  $U$ ), для  $e = 2$  — через  $t''$ ,  $u''$ , для  $e = 3$  — через  $t'''$ ,  $u'''$  и т. д., и докажем, что если брать для  $e$  все неотрицательные целые числа, т. е.  $0$  и все положительные числа от  $1$  до  $\infty$ , то эти выражения дадут все положительные значения  $t$ ,  $u$ , а именно: (I) что все значения этих выражений действительно являются значениями  $t$ ,  $u$ ; (II) что все эти значения являются целыми числами; (III) что не существует положительных значений  $t$ ,  $u$ , которые не содержали бы в этих формулах.

I. Если вместо  $t^{(e)}$ ,  $u^{(e)}$  подставить их значения, то при помощи равенства [1] без труда устанавливается, что

$$(t^{(e)} + u^{(e)} \sqrt{D})(t^{(e)} - u^{(e)} \sqrt{D}) = m^2, \text{ т. е. } t^{(e)2} - Du^{(e)2} = m^2.$$

II. Таким же образом легко устанавливается, что

$$t^{(e+1)} + t^{(e-1)} = \frac{2T}{m} t^{(e)}, \quad u^{(e+1)} + u^{(e-1)} = \frac{2T}{m} u^{(e)}.$$

Отсюда вытекает, что оба ряда  $t^0, t', t'', t''', \dots; u^0, u', u'', u''', \dots$  являются рекуррентными, именно,

$$t'' = \frac{2T}{m} t' - t^0, \quad t''' = \frac{2T}{m} t'' - t', \dots; \quad u'' = \frac{2T}{m} u' - u^0, \dots$$

Так как теперь, по предположению существует некоторая форма  $(M, N, P)$  с определителем  $D$ , у которой  $M, 2N, P$  делятся на  $m$ , мы имеем

$$T^2 = (N^2 - MP)U^2 + m^2,$$

и потому  $4T^2$ , очевидно, делится на  $m^2$ . Поэтому  $2T/m$  является целым и притом положительным числом. Так как, однако,  $t^0 = m$ ,  $t' = T$ ,  $u^0 = 0$ ,  $u' = U$ , и потому эти числа целые, то будут целыми также и все числа  $t'', t''', \dots, u'', u''', \dots$ . Далее, очевидно, так как  $T^2 > m^2$ , что все  $t^0, t', t'', t''', \dots$  положительны и непрерывно возрастают до бесконечности, и точно так же — все  $u^0, u', u'', u''', \dots$ .

III. Если мы предположим, что существуют еще и другие положительные значения  $t, u$ , которые не содержатся в рядах  $t^0, t', t'', \dots, u^0, u', u'', \dots$ , например,  $\mathfrak{Z}, \mathfrak{U}$ , то так как ряд  $u^0, u', \dots$  возрастает от 0 до бесконечности, очевидно, что  $\mathfrak{U}$  обязательно будет лежать между двумя соседними членами  $u^{(n)}$  и  $u^{(n+m)}$ , так что  $\mathfrak{U} > u^{(n)}$  и  $\mathfrak{U} < u^{(n+1)}$ . Чтобы доказать невозможность этого предположения, сделаем следующие замечания.

1. Уравнение  $t^2 - Du^2 = m^2$  также будет удовлетворяться, если положить

$$t = \frac{1}{m} (\mathfrak{Z}t^{(n)} - D\mathfrak{U}u^{(n)}), \quad u = \frac{1}{m} (\mathfrak{U}t^{(n)} - \mathfrak{Z}u^{(n)}).$$

Это легко может быть установлено простой подстановкой; а то, что эти значения, которые мы для краткости обозначим через  $\tau, \upsilon$ , всегда являются целыми числами, мы докажем следующим образом. Если  $(M, N, P)$  — форма с определителем  $D$ , и  $m$  — наибольший общий делитель чисел  $M, 2N, P$ , то на  $m$  будут делиться как  $\mathfrak{Z} + N\mathfrak{U}$ , так и  $t^{(n)} + Nu^{(n)}$  и потому также  $\mathfrak{U}(t^{(n)} + Nu^{(n)}) - u^{(n)}(\mathfrak{Z} + N\mathfrak{U})$  или  $\mathfrak{U}t^{(n)} - \mathfrak{Z}u^{(n)}$ . Поэтому  $\upsilon$  будет целым числом, а тем самым также и  $\tau$ , ибо  $\tau^2 = D\upsilon^2 + m^2$ .

2. Очевидно, что  $\upsilon$  не может быть равно нулю, так как из этого следовало бы, что

$$\mathfrak{U}^2 t^{(n)^2} = \mathfrak{I}^2 u^{(n)^2},$$

или

$$\mathfrak{U}^2 (Du^{(n)^2} + m^2) = u^{(n)^2} (D\mathfrak{U}^2 + m^2),$$

или  $\mathfrak{U}^2 = u^{(n)^2}$ , вопреки предположению, что  $\mathfrak{U} > u^{(n)}$ . Так как, за исключением значения 0, наименьшее значение  $u$  равно  $U$ , то  $\upsilon$ , очевидно, не меньше чем  $U$ .

3. Из значений  $t^{(n)}$ ,  $t^{(n+1)}$ ,  $u^{(n)}$ ,  $u^{(n+1)}$  легко может быть установлено, что

$$mU = u^{(n+1)}t^{(n)} - t^{(n+1)}u^{(n)}.$$

Поэтому  $\mathfrak{U}t^{(n)} - \mathfrak{I}u^{(n)}$  заведомо не меньше, чем  $u^{(n+1)}t^{(n)} - t^{(n+1)}u^{(n)}$ .

4. Теперь из равенства  $\mathfrak{I}^2 - D\mathfrak{U}^2 = m^2$  получаем

$$\frac{\mathfrak{I}}{\mathfrak{U}} = \sqrt{D + \frac{m^2}{\mathfrak{U}^2}},$$

и аналогично

$$\frac{t^{(n+1)}}{u^{(n+1)}} = \sqrt{D + \frac{m^2}{u^{(n+1)^2}}},$$

откуда легко следует, что  $\frac{\mathfrak{I}}{\mathfrak{U}} > \frac{t^{(n+1)}}{u^{(n+1)}}$ . А отсюда и из следствия 3 получаем

$$(\mathfrak{U}t^{(n)} - \mathfrak{I}u^{(n)}) \left( t^{(n)} + u^{(n)} \frac{\mathfrak{I}}{\mathfrak{U}} \right) > (u^{(n+1)}t^{(n)} - t^{(n+1)}u^{(n)}) \left( t^{(n)} + u^{(n)} \frac{t^{(n+1)}}{u^{(n+1)}} \right),$$

или, если раскрыть скобки и вместо  $\mathfrak{I}^2$ ,  $t^{(n)^2}$ ,  $t^{(n+1)^2}$  подставить их значения  $D\mathfrak{U} + m^2$ ,  $Du^{(n)^2} + m^2$ ,  $Du^{(n+1)^2} + m^2$ ,

$$\frac{1}{\mathfrak{U}} (\mathfrak{U}^2 - u^{(n)^2}) > \frac{1}{u^{(n+1)}} (u^{(n+1)^2} - u^{(n)^2}),$$

откуда, так как каждая величина, очевидно, положительна, посредством перестановки следует, что

$$\mathfrak{U} + \frac{u^{(n)^2}}{u^{(n+1)}} > u^{(n+1)} + \frac{u^{(n)^2}}{\mathfrak{U}}.$$

Это, однако, невозможно, так как первый член первой величины меньше первого члена второй, и точно так же второй член первой величины меньше второго члена второй величины. Поэтому наше предположение не может выполняться, и ряды  $t^0, t', t'', \dots, u^0, u', u'', \dots$  представляют все положительные значения  $t, u$ .

**Пример.** Для  $D = 61$ ,  $m = 2$  в качестве наименьших положительных значений  $t, u$  мы нашли следующие: 1523, 195. Поэтому все положительные значения будут представляться следующими формулами:

$$t = \left(\frac{1523}{2} + \frac{195}{2} \sqrt{61}\right)^e + \left(\frac{1523}{2} - \frac{195}{2} \sqrt{61}\right)^e,$$

$$u = \frac{1}{\sqrt{61}} \left[ \left(\frac{1523}{2} + \frac{195}{2} \sqrt{61}\right)^e - \left(\frac{1523}{2} - \frac{195}{2} \sqrt{61}\right)^e \right].$$

При этом мы находим

$$t^0 = 2, \quad t' = 1523, \quad t'' = 1523 t' - t^0 = 2319527,$$

$$t''' = 1523 t'' - t' = 3532618098, \dots;$$

$$u^0 = 0, \quad u' = 195, \quad u'' = 1523 u' - u^0 = 296985,$$

$$u''' = 1523 u'' - u' = 452307960, \dots$$

## 201

Относительно рассмотренной в предыдущем пункте проблемы мы добавим еще следующие замечания.

1. После того как мы показали, как во всех случаях можно решить уравнение  $t^2 - Du^2 = m^2$ , где  $m$  — наибольший общий делитель трех чисел  $M, 2N, P$  с тем свойством, что  $N^2 - MP = D$ , стоит потрудиться над тем, чтобы определить все числа, которые могут быть таким делителем, т. е. все значения  $m$  для заданного значения  $D$ . Положим  $D = n^2 D'$ , где  $D'$  полностью свободно от квадратных сомножителей, что достигается, если за  $n^2$  взять наибольший квадрат, входящий в  $D$ ; если же  $D$  само уже не делится ни на какой квадратный сомножитель, то нужно положить  $n = 1$ . Тогда мы утверждаем следующее.

*Во-первых.* Если  $D'$  имеет вид  $4k + 1$ , то каждый делитель числа  $2n$  является значением  $m$ , и обратно. Действительно, если  $g$  —

делитель числа  $2n$ , то мы получаем форму  $(g, n, n^2(1 - D')/g)$ , определитель которой равен  $D$  и у которой наибольший общий делитель чисел  $g, 2n, n^2(D' - 1)/g$ , очевидно, равен  $g$  (так как  $\frac{n^2(D' - 1)}{g^2} = \frac{4n^2}{g^2} \cdot \frac{D' - 1}{4}$ , очевидно, является целым числом). Если же, наоборот, предположить, что  $g$  есть значение  $m$ , именно, наибольший общий делитель чисел  $M, 2N, P$  и  $N^2 - MP = D$ , то очевидно, что  $4D$  или  $4n^2D'$  будет делиться на  $g^2$ . Отсюда, однако, следует, что  $2n$  обязательно делится на  $g$ . Действительно, если бы  $g$  не входило в  $2n$ , то  $g$  и  $2n$  имели бы наибольший общий делитель, который меньше чем  $g$ , и если он равен  $\delta$  и  $2n = \delta n', g = \delta g'$ , то  $n'^2D'$  делилось бы на  $g'^2$ ,  $n'$  было бы взаимно просто с  $g'$  и потому также  $n'^2$  — с  $g'^2$ , а значит,  $D'$  также делилось бы на  $g'^2$ , вопреки предположению, по которому  $D'$  свободно от всякого квадратного сомножителя.

*Во-вторых.* Если  $D'$  имеет вид  $4k + 2$  или  $4k + 3$ , то каждый делитель числа  $n$  является значением  $m$ , и обратно, каждое значение  $m$  входит в  $n$ . Действительно, если  $g$  есть делитель  $n$ , то мы получаем форму  $(g, 0, -n^2D'/g)$ , определитель которой равен  $D$  и у которой наибольший общий делитель чисел  $g, 0, n^2D'/g$ , очевидно, равен  $g$ . Если же мы предположим, что  $g$  есть значение  $m$ , именно, наибольший общий делитель чисел  $M, 2N, P$  и  $N^2 - MP = D$ , то так же, как и выше,  $g$  входит в  $2n$ , или  $2n/g$  является целым числом. Если бы это отношение было нечетным, то имело бы место  $\frac{4n^2}{g^2} \equiv 1 \pmod{4}$ , и потому  $4n^2D'/g^2$  было бы или  $\equiv 2$ , или  $\equiv 3 \pmod{4}$ . Но  $\frac{4n^2D'}{g^2} = \frac{4D}{g^2} = \frac{4N^2}{g^2} - \frac{4MP}{g^2} \equiv \frac{4N^2}{g^2} \pmod{4}$ , и потому  $4N^2/g^2$  или  $\equiv 2$  или  $\equiv 3 \pmod{4}$ . Это, однако, невозможно, так как каждый квадрат должен быть сравним по модулю 4 или с нулем, или с единицей. Следовательно, отношение  $2n/g$  обязательно четно и тем самым число  $n/g$  целое, т. е.  $g$  есть делитель  $n$ .

Таким образом, отсюда вытекает, что 1 всегда является значением  $m$ , или что уравнение  $t^2 - Du^2 = 1$  для каждого положительного неквадратного значения  $D$  разрешимо; далее, что 2 только тогда является значением  $m$ , когда  $D$  имеет или вид  $4k$ , или вид  $4k + 1$ .

2. Если  $m > 2$ , но при этом является допустимым числом, то решение уравнения  $t^2 - Du^2 = m^2$  может быть сведено к решению подобного уравнения, в котором  $m$  равно 1 или 2. Если, как и перед этим, положить  $D = n^2 D'$ , то если  $m$  входит в  $n$ ,  $m^2$  будет входить в  $D$ . Если предположить тогда, что наименьшие значения  $p, q$  в уравнении  $p^2 - \frac{D}{m^2} q^2 = 1$  суть  $p = P, q = Q$ , то наименьшие значения  $t, u$  в уравнении  $t^2 - Du^2 = m^2$  будут  $t = mP, u = Q$ . Если же  $m$  не входит в  $n$ , то оно обязательно будет входить в  $2n$  и, очевидно, будет четным; а  $4D/m^2$  есть целое число. И если тогда в качестве наименьших значений  $p, q$  в уравнении  $p^2 - \frac{4D}{m^2} q^2 = 4$  найдены значения  $p = P, q = Q$ , то наименьшими значениями  $t, u$  в уравнении  $t^2 - Du^2 = m^2$  будут  $t = \frac{m}{2} P, u = Q$ . В обоих случаях, однако, не только из наименьших значений  $p, b$  могут быть выведены наименьшие значения  $t, u$ , но, очевидно, что тем же методом из всех значений первых могут быть получены все значения вторых.

3. Если, как в предыдущем пункте,  $t^0, u^0, t', u' : t'', u''; \dots$  обозначают все положительные значения  $t, u$  в уравнении  $t^2 - Du^2 = m^2$ , и оказывается, что некоторые значения из этих рядов сравнимы по некоторому данному модулю  $r$  с первыми значениями этих же рядов, например,  $t^{(\rho)} \equiv t^0$  (или  $\equiv m$ ),  $u^{(\rho)} \equiv u^0$  (или  $\equiv 0$ )  $(\text{mod } r)$  и одновременно следующие значения сравнимы со вторыми значениями, именно,  $t^{(\rho+1)} \equiv t', u^{(\rho+1)} \equiv u' \pmod{r}$ , то также

$$t^{(\rho+2)} \equiv t'', u^{(\rho+2)} \equiv u''; t^{(\rho+3)} \equiv t''', u^{(\rho+3)} \equiv u''', \dots$$

Это легко следует из того, что каждый из двух рядов  $t^0, t', t'', \dots; u^0, u', u'', \dots$  является рекуррентным; действительно, так как

$$t'' = \frac{2T}{m} t' - t^0, t^{(\rho+2)} = \frac{2T}{m} t^{(\rho+1)} - t^{(\rho)},$$

то также

$$t'' \equiv t^{(\rho+2)},$$

и точно так же для остальных значений. Отсюда следует, что вообще

$$t^{(h+\rho)} \equiv t^{(h)}, u^{(h+\rho)} \equiv u^{(h)} \pmod{r},$$

где  $h$  обозначает любое число, и еще более общо, что если

$$\mu \equiv \nu \pmod{\rho}, \text{ то также } t^{(\mu)} \equiv t^{(\nu)}, u^{(\mu)} \equiv u^{(\nu)} \pmod{r}.$$

4. Упомянутым в предыдущем замечании условиям всегда можно удовлетворить, именно, для любого заданного модуля  $r$  всегда может быть найден индекс  $\rho$ , для которого

$$t^{(\rho)} \equiv t^0, \quad t^{(\rho+1)} \equiv t', \quad u^{(\rho)} \equiv u^0, \quad u^{(\rho+1)} \equiv u'.$$

Чтобы это доказать, заметим следующее.

*Во-первых*, третьему условию можно удовлетворить всегда. Действительно, из данных в замечании 1 критериев без труда устанавливается, что уравнение  $p^2 - r^2 Dq^2 = m^2$  также разрешимо, и если предположить, что наименьшими значениями  $p, q$  (кроме  $m, 0$ ) являются  $P, Q$ , то среди значений  $t, u$ , очевидно, найдутся также и  $t = P, u = rQ$ . Поэтому  $P, rQ$  будут содержаться в рядах  $t^0, t', \dots; u^0, u', \dots$ , и если  $P = t^{(\lambda)}, rQ = u^{(\lambda)}$ , то будет  $u^{(\lambda)} \equiv 0 \equiv u^0 \pmod{r}$ . Кроме того, легко видеть, что между  $u^0$  и  $u^{(\lambda)}$  не будет ни одного члена, который сравним с  $u^0$  по модулю  $r$ .

*Во-вторых*, ясно, что если, кроме того, здесь выполнены и три остальные условия, именно, если также  $u^{(\lambda+1)} \equiv u', t^{(\lambda)} \equiv t^0, t^{(\lambda+1)} \equiv t'$ , то нужно только положить  $\rho = \lambda$ . Если же то или иное из этих условий не имеет места, то я утверждаю, что наверняка можно положить  $\rho = 2\lambda$ . Действительно, из равенства [1] и общих формул для  $t^{(e)}, u^{(e)}$  предыдущего пункта следует, что

$$t^{(2\lambda)} = \frac{1}{m} (t^{(\lambda)2} + Du^{(\lambda)2}) = \frac{1}{m} (m^2 + 2Du^{(\lambda)2}),$$

и потому

$$\frac{t^{(2\lambda)} - t^0}{r} = \frac{2Du^{(\lambda)2}}{mr},$$

причем эта величина является целым числом, так как по предположению  $r$  входит в  $u^{(\lambda)}$  и точно также  $m^2$  — в  $4D$ , а потому и подавно  $m$  — в  $2D$ . Далее,  $u^{(2\lambda)} = \frac{2}{m} t^{(\lambda)} u^{(\lambda)}$ , и так как

$$4t^{(\lambda)2} = 4Du^{(\lambda)2} + 4m^2,$$



и потому делится на  $m^2$ , то и  $2t^{(\lambda)}$  делится на  $m$  и тем самым  $u^{(2\lambda)}$  делится на  $r$  или

$$u^{(2\lambda)} \equiv u^0 \pmod{r}.$$

*В-третьих*, находим

$$t^{(2\lambda+1)} = t' + \frac{2Du^{(\lambda)}u^{(\lambda+1)}}{m},$$

и так как по аналогичной причине число  $2Du^{(\lambda)} / mr$  целое, то

$$t^{(2\lambda+1)} \equiv t' \pmod{r}.$$

*Наконец*, находим

$$u^{(2\lambda+1)} = u' + \frac{2t^{(\lambda+1)}u^{(\lambda)}}{m},$$

и так как  $2t^{(\lambda+1)}$  делится на  $m$ , и  $u^{(\lambda)}$  делится на  $r$ , то

$$u^{(2\lambda+1)} \equiv u' \pmod{r}.$$

Впрочем, польза двух последних замечаний обнаружится в дальнейшем.

## 202

Специальный случай проблемы, именно, решение уравнения  $t^2 - Du^2 = 1$ , рассматривался уже математиками предшествующего столетия. Остроумный Ф е р м а задал эту проблему английским аналитикам, и В а л л и с называет Б р у н к е р а, как нашедшего решение, которое он приводит в своей «*Algebra Kapitel*», p. 98 и «*Opera*», T. II, p. 418 и сл.; О з а н а м называет таковым Ф е р м а, и, наконец, Э й л е р (который рассматривал этот вопрос в «*Comm. Petr.*», VI, p. 175; «*Comm. nov.*», XI, p. 28; «*Algebra*» \*, *Pars II*, p. 226; «*Opusc. Analyt.*», I, p. 310) — англичанина П е л л я, вследствие чего эта проблема некоторыми авторами называется *проблемой*

---

\* В этом сочинении для изложенного в п. 27 алгоритма применяются такие же обозначения, о чем мы в своем месте забыли упомянуть.

П е л л я. Все эти решения по существу совпадают с тем, которое получится, если в п. 198 использовать такую приведенную форму, у которой  $a = 1$ . Однако то, что предписываемые операции рано или поздно обязательно придут к концу, т. е. что проблема действительно всегда разрешима, никто не доказал строго\* до Л а г р а н ж а «*Mélanges de la Soc. de Turin*», T. IV, p. 19, и более коротко в «*Hist. de l'Ac. de Berlin*», 1767, p. 237. Это исследование находится также в уже указанных дополнениях к «Алгебре» Э й л е р а. Впрочем, наш метод (который основывается на совершенно других принципах и не ограничивается случаем  $m = 1$ ) дает намного больше путей для получения решения, так как в п. 198 мы ведь можем исходить и из любой другой приведенной формы  $(a, b, -a')$ .

## 203

**Задача.** Пусть формы  $\Phi, \phi$  эквивалентны; требуется представить все преобразования одной из них в другую.

**Решение.** Если эти формы эквивалентны только одним способом (т. е. или только собственно или только несобственно), то найдем в соответствии с п. 196 одно преобразование формы  $\phi$  в  $\Phi$ , которое пусть будет  $\alpha, \beta, \gamma, \delta$ ; очевидно, что не может быть других преобразований, кроме однотипных с ним. Если же  $\phi, \Phi$  эквивалентны как собственно, так и несобственно, то найдем два неоднотипных преобразования, т. е. одно собственное и одно несобственное, например,  $\alpha, \beta, \gamma, \delta$  и  $\alpha', \beta', \gamma', \delta'$ ; любое другое преобразование будет однотипным или с первым, или со вторым. Если поэтому форма  $\phi$  равна  $(a, b, c)$ , ее определитель равен  $D$ , наибольший общий делитель чисел  $a, 2b, c$  (как и все время до сих пор) равен  $m$ , и  $t, u$  — всевозможные числа, удовлетворяющие уравнению  $t^2 - Du^2 = m^2$ ,

---

\* То, что в указанном сочинении (стр. 427, 428) говорит об этом В а л л и с, не убедительно. Ошибка состоит в том, что он предполагает, что если задана величина  $p$ , то можно найти целые числа  $z, a$  с тем свойством, что  $z/a$  меньше чем  $p$ , однако разность меньше, чем некоторое определенное число. Это верно в том случае, если это число постоянно, но здесь как раз оно зависит от  $a$  и  $z$ , и потому переменнo.

то в первом случае все преобразования формы  $\varphi$  в  $\Phi$  будут содержаться в формулах (I), а во втором случае — в формулах (I) и (II):

$$\begin{aligned} \text{(I)} \quad & \left\{ \frac{1}{m} [\alpha t - (\alpha b + \gamma c) u], \quad \frac{1}{m} [\beta t - (\beta b + \delta c) u], \right. \\ & \left. \frac{1}{m} [\gamma t + (\alpha a + \gamma b) u], \quad \frac{1}{m} [\delta t + (\beta a + \delta b) u]; \right. \\ \text{(II)} \quad & \left\{ \frac{1}{m} [\alpha' t - (\alpha' b + \gamma' c) u], \quad \frac{1}{m} [\beta' t - (\beta' b + \delta' c) u], \right. \\ & \left. \frac{1}{m} [\gamma' t + (\alpha' a + \gamma' b) u], \quad \frac{1}{m} [\delta' t + (\beta' a + \delta' b) u]. \right. \end{aligned}$$

**Пример.** Мы хотим иметь все преобразования формы (129, 92, 65) в форму (42, 59, 81). То, что они эквивалентны только несобственно, мы нашли в п. 195, а в следующем пункте мы получили несобственное преобразование первой формы во вторую: —47, —56, 73, 87.

Поэтому все преобразования формы (129, 92, 65) в форму (42, 59, 81) представляются формулами

$$-(47t + 421u), \quad -(56t + 503u), \quad 73t + 653u, \quad 87t + 780u,$$

где  $t, u$  обозначают всевозможные числа, удовлетворяющие уравнению  $t^2 - 79u^2 = 1$ . Эти числа представляются формулами

$$\begin{aligned} \pm t &= \frac{1}{2} [(80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e], \\ \pm u &= \frac{1}{2\sqrt{79}} [(80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e], \end{aligned}$$

где для  $e$  нужно брать все целые неотрицательные числа.

Очевидно, что формулы, представляющие все преобразования, будут тем проще, чем проще исходное преобразование, из которого эти формулы выведены. То, из какого преобразования исходить, зависит от нашего желания; поэтому общие формулы часто могут быть сделаны проще, если из первоначально найденных формул мы сначала получим более простое преобразование, придав  $t, u$  определенные значения, а затем составим для этого преобразования как исходного новые формулы. Так, например, если в найденных в пре-

дыдущем пункте формулах положить  $t = 80$ ,  $u = -9$ , то получится более простое преобразование, чем то, из которого мы исходили, именно, получится  $29$ ,  $47$ ,  $-37$ ,  $-60$ , откуда получаются общие формулы  $29t - 263u$ ,  $47t - 424u$ ,  $-37t + 337u$ ,  $-60t + 543u$ . Таким образом, если по предыдущим правилам установлены общие формулы, то можно посмотреть, нельзя ли, придавая  $t$ ,  $u$  определенные значения  $\pm t'$ ,  $\pm u'$ ;  $\pm t''$ ,  $\pm u''$ ; ..., получить более простое преобразование, чем то, из которого формулы были выведены, и если можно, то из этого преобразования могут быть выведены более простые формулы.

Впрочем, при суждении о простоте остается некоторый произвол, который мы при желании могли бы ввести в твердые рамки и вместе с тем указать в ряде  $t'$ ,  $u'$ ;  $t''$ ,  $u''$ ; ... границу, за пределами которой преобразования постоянно будут менее простыми, так что дальше заходить уже не нужно, а следует произвести исследование только до этой границы. Так как, однако, при пользовании предписанными правилами простейшее преобразование в большинстве случаев получается или тотчас же, или при применении для  $t$ ,  $u$  значений  $\pm t'$ ,  $\pm u'$ , то мы ради краткости это исследование опустим.

## 205

**Задача.** *Найти все представления заданного числа  $M$  заданной формой  $ax^2 + 2bxy + cy^2$  с положительным неквадратным определителем  $D$ .*

**Решение.** Заметим сначала, что получение представлений с взаимно простыми значениями  $x$ ,  $y$  здесь, как и выше (п. 181) для форм с отрицательным определителем, может быть сведено к тому случаю, когда ищутся представления со взаимно простыми значениями неизвестных, и было бы излишне это здесь повторять. Для возможности же представления посредством взаимно простых значений  $x$ ,  $y$  необходимо, чтобы  $D$  было квадратичным вычетом по модулю  $M$ , и если всевозможные значения выражения  $\sqrt{D} \pmod{M}$  суть  $N$ ,  $-N$ ,  $N'$ ,  $-N'$ ,  $N''$ ,  $-N''$ , ... (относительно которых мы можем предполагать, что ни одно из них не больше чем  $M/2$ ), то каждое представление числа  $M$  заданной формой будет принадлежать одному

из этих значений. Поэтому прежде всего должны быть определены эти значения, а затем найдены принадлежащие отдельным значениям представления. Представления, которые принадлежат значению  $N$ , могут быть только тогда, когда формы  $(a, b, c)$  и  $(M, N, \frac{N^2-D}{M})$  собственно эквивалентны; если это имеет место, то найдем какое-нибудь собственное преобразование первой формы во вторую, например,  $\alpha, \beta, \gamma, \delta$ . Тогда в качестве принадлежащего значению  $N$  представления числа  $M$  формой  $(a, b, c)$  получаем следующее:  $x = \alpha, y = \gamma$ , и все принадлежащие этому значению представления могут быть представлены формулой

$$x = \frac{1}{m} [\alpha t - (\alpha b + \gamma c) u], \quad y = \frac{1}{m} [\gamma t + (\alpha a + \gamma b) u],$$

где  $m$  обозначает наибольший общий делитель чисел  $a, 2b, c$ , а  $t, u$  — произвольные числа, удовлетворяющие уравнению  $t^2 - Du^2 = m^2$ . Впрочем, эта общая формула, очевидно, может быть сделана тем проще, чем проще преобразование  $\alpha, \beta, \gamma, \delta$ , из которого она выводилась; поэтому будет не лишним предварительно найти в соответствии с предыдущим пунктом простейшее преобразование формы  $(a, b, c)$  в  $(M, N, (N^2-D)/M)$ , и выводить формулу из него.

Точно таким же образом могут быть указаны представления, принадлежащие остальным значениям  $-N, N', -N', \dots$  в виде общих формул (если такие представления вообще существуют).

**Пример.** Найдем все представления числа 585 формой  $42x^2 + 62xy + 21y^2$ . Что касается представлений с не взаимно простыми значениями  $x, y$ , то тотчас же ясно, что таковых не может быть, кроме таких, у которых наибольший общий делитель  $x, y$  равен 3, так как 585 делится только на квадрат, равный 9. Если поэтому найдены все представления числа  $\frac{585}{9} = 65$  формой  $42x'^2 + 62x'y' + 21y'^2$ , у которых  $x'$  взаимно просто с  $y'$ , то все представления числа 585 формой  $42x^2 + 62xy + 21y^2$ , у которых  $x$  не взаимно просто с  $y$ , будут получены, если положить  $x = 3x', y = 3y'$ . Значения выражения  $\sqrt{79} \pmod{65}$  суть  $\pm 12, \pm 27$ . В качестве представления числа 65, которое принадлежит значению  $-12$ , находим  $x' = 2, y' = -1$ ; поэтому все принадлежащие этому значению представления числа 65

будут охватываться формулой  $x' = 2t - 41u$ ,  $y' = -t + 53u$ , и тем самым все получающиеся отсюда представления числа 585 — формулой  $x = 6t - 123u$ ,  $y = -3t + 159u$ . Подобным же образом находим в качестве формулы, которая выражает все принадлежащие значению  $+12$  представления числа 65, следующую:  $x' = 22t - 199u$ ;  $y' = -23t - 211u$ , и в качестве формулы, которая охватывает все получающиеся отсюда представления числа 585, следующую:  $x = 66t - 597u$ ,  $y = -69t + 633u$ . Значениям же  $+27$  и  $-27$  не принадлежит ни одно представление числа 65. Чтобы найти представления числа 585 со взаимно простыми значениями  $x$ ,  $y$ , нужно сначала получить значения выражения  $\sqrt{79} \pmod{585}$ , которые суть  $\pm 77$ ,  $\pm 103$ ,  $\pm 157$ ,  $\pm 248$ . Находим, что значениям  $\pm 77$ ,  $\pm 103$ ,  $\pm 248$  не принадлежит ни одно представление; значению же  $-157$  принадлежит представление  $x = 3$ ,  $y = 1$ , из которого в качестве общей формулы, которая дает все принадлежащие этому значению представления, выводим следующую:  $x = 3t - 114u$ ,  $y = t + 157u$ . Подобным же образом находим в качестве принадлежащего значению  $+157$  представления  $x = 83$ ,  $y = -87$ , и в качестве формулы, в которой содержатся все подобные представления, следующую:  $x = 83t - 746u$ ,  $y = -87t + 789u$ . Мы получаем, таким образом, четыре общие формулы, в которых содержатся все представления числа 585 формой  $42x^2 + 62xy + 21y^2$ , именно

$$\begin{aligned} x &= 6t - 123u, & y &= -3t + 159u; \\ x &= 66t - 597u, & y &= -69t + 633u; \\ x &= 3t - 114u, & y &= t + 157u; \\ x &= 83t - 746u, & y &= -87t + 789u, \end{aligned}$$

причем  $t$ ,  $u$  обозначают произвольные целые числа, которые удовлетворяют уравнению  $t^2 - 79u^2 = 1$ .

На специальных применениях этих исследований о формах с положительным неквадратным определителем мы, ради краткости, не останавливаемся, так как каждое из них без труда может быть получено так же, как и в пп. 176, 182, и немедленно переходим к единственно еще остающимся формам с положительным квадратным определителем.

## О формах с квадратным определителем

206

**Задача.** Пусть задана форма  $(a, b, c)$  с квадратным определителем  $h^2$ , где  $h$  обозначает положительное значение корня; требуется найти собственно эквивалентную ей форму  $(A, B, C)$ , у которой  $A$  лежит между границами 0 и  $2h - 1$  (включительно),  $B = h$  и  $C = 0$ .

**Решение I.** Так как  $h^2 = b^2 - ac$ , то  $(h - b) : a = c : [-(h + b)]$ , пусть этому отношению равно отношению  $\beta : \delta$  где  $\beta$  взаимно просто с  $\delta$ ; определим  $\alpha, \gamma$  так, что  $\alpha\delta - \beta\gamma = 1$ , что возможно. Пусть подстановкой  $\alpha, \beta, \gamma, \delta$  форма  $(a, b, c)$  переводится в форму  $(a', b', c')$ , которая тем самым собственно эквивалентна первой. При этом мы имеем

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = \\ &= (h - b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h + b)\beta\gamma = \\ &= h(\alpha\delta - \beta\gamma) = h; \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 = \\ &= (h - b)\beta\delta + 2b\beta\delta - (h + b)\beta\delta = 0. \end{aligned}$$

Если поэтому, кроме того,  $a'$  уже лежит между границами 0 и  $2h - 1$ , то форма  $(a', b', c')$  будет удовлетворять всем условиям.

II. Если же  $a'$  лежит вне границ 0 и  $2h - 1$ , то пусть  $A$  — наименьший положительный вычет числа  $a'$  по модулю  $2h$ , который, очевидно, будет лежать между этими границами; положим  $A - a' = 2hk$ . Тогда форма  $(a', b', c')$ , т. е.  $(a', h, 0)$  будет при собственной подстановке 1, 0,  $k$ , 1 переходить в форму  $(A, h, 0)$ , которая собственно эквивалентна формам  $(a', b', c')$  и  $(a, b, c)$  и удовлетворяет всем условиям. Заметим, что форма  $(a, b, c)$  переходит в форму  $(A, h, 0)$  при подстановке  $\alpha + \beta k, \beta, \gamma + \delta k, \delta$ .

**Пример.** Пусть дана форма  $(27, 15, 8)$ , определитель которой равен 9. Здесь  $h = 3$ ; далее, отношениям  $-12 : 27 = 8 : (-18)$  в наименьших числах равно отношение  $4 : (-9)$ . Если, таким образом, положить  $\beta = 4, \delta = -9, \alpha = -1, \gamma = 2$ , то форма  $(a', b', c')$  будет следующая:  $(-1, 3, 0)$ ; она переходит при подстановке 1, 0, 1, 1 в форму  $(5, 3, 0)$ . Последняя является, таким образом,

искомой формой, и заданная форма переходит в нее при собственной подстановке 3, 4, — 7, — 9.

Такие формы  $(A, B, C)$ , у которых  $C = 0$ ,  $B = h$  и  $A$  лежит между границами 0 и  $2h - 1$ , мы будем называть приведенными формами; их, таким образом, следует отличать от приведенных форм с отрицательным определителем и положительным неквадратным определителем.

## 207

**Теорема.** Две не совпадающие приведенные формы  $(a, h, 0)$  и  $(a', h, 0)$  не могут быть собственно эквивалентны.

**Доказательство.** Действительно, предположим, что они собственно эквивалентны и первая переходит во вторую при собственной подстановке  $\alpha, \beta, \gamma, \delta$ ; тогда имеем четыре равенства

$$[1] \quad a\alpha^2 + 2h\alpha\gamma = a',$$

$$[2] \quad a\alpha\beta + h(\alpha\delta + \beta\gamma) = h,$$

$$[3] \quad a\beta^2 + 2h\beta\delta = 0,$$

$$[4] \quad \alpha\delta - \beta\gamma = 1.$$

Если умножить второе равенство на  $\beta$ , третье — на  $\alpha$  и вычесть, то получится —  $h(\alpha\delta - \beta\gamma)\beta = \beta h$ , или, в силу [4], —  $\beta h = \beta h$ , так что обязательно  $\beta = 0$ . Поэтому из [4] следует, что  $\alpha\delta = 1$  и  $\alpha = \pm 1$ . Тем самым из [1] вытекает, что  $a \pm 2h\gamma = a'$ . Но это равенство может выполняться только в том случае, если  $\gamma = 0$  (так как, по предположению,  $a$  и  $a'$  оба лежат между границами 0 и  $2h$ ), т. е. если  $a = a'$ , или если формы  $(a, h, 0)$  и  $(a', h, 0)$  совпадают, что противоречит предположению.

Поэтому следующие задачи, которые для неквадратного определителя представляют едва ли не наибольшие трудности, могут быть решены без труда.

I. Если даны две формы  $F, F'$  с одинаковым квадратным определителем, то нужно узнать, являются ли они собственно эквивалентными. Найдем две приведенные формы, собственно эквивалентные соответственно формам  $F, F'$ ; если они совпадают, то заданные формы собственно эквивалентны; в противном же случае — нет.



II. При тех же предположениях нужно определить, являются ли формы несобственно эквивалентными. Пусть формой, противоположной одной из заданных форм, например  $F$ , является форма  $G$ ; если она собственно эквивалентна форме  $F'$ , то  $F$  и  $F'$  будут несобственно эквивалентными, и обратно.

## 208

**Задача.** Пусть даны две собственно эквивалентные формы  $F$ ,  $F'$  с определителем  $h^2$ ; найти собственное преобразование одной из них в другую.

**Решение.** Пусть форме  $F$  собственно эквивалентна приведенная форма  $\Phi$ , которая в силу предположения будет тем самым собственно эквивалентна также и форме  $F'$ . Найдем, согласно п. 206, собственное преобразование формы  $F$  в  $\Phi$ , которое обозначим через  $\alpha, \beta, \gamma, \delta$ , и точно так же — собственное преобразование формы  $F'$  в  $\Phi$ , которое обозначим через  $\alpha', \beta', \gamma', \delta'$ . Тогда  $\Phi$  будет переходить в  $F'$  при собственной подстановке  $\delta', -\beta', -\gamma', \alpha'$ , и потому  $F$  будет переходить в  $F'$  при собственной подстановке

$$\alpha\delta' - \beta\gamma', \beta\alpha' - \alpha\beta', \gamma\delta' - \delta\gamma', \delta\alpha' - \gamma\beta'.$$

Стоит потратить усилия на то, чтобы получить для этого преобразования формы  $F$  в  $F'$  другую формулу, для которой не нужно предварительно знать приведенной формы  $\Phi$ . Предположим, что

$$F = (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0).$$

Так как отношению  $(h - b) : a$  или  $c : [-(h + b)]$  равно отношению в наименьших числах  $\beta : \delta$ , то легко видеть, что  $\frac{h - b}{\beta} = \frac{a}{\delta}$  есть целое число, которое мы положим равным  $f$ ; точно так же  $\frac{c}{\beta} = \frac{-h - \beta}{\delta}$  является целым числом, которое мы положим равным  $g$ . Но мы имеем  $A = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$  и потому  $\beta A = a\alpha^2\beta + 2b\alpha\beta\gamma + c\beta\gamma^2$ , или (если заменить  $\alpha\beta$  на  $\delta(h - b)$  и  $c$  — на  $\beta\gamma$ )

$$\beta A = \alpha^2\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta^2\gamma^2g,$$

или (вследствие того, что  $b = -h - \delta g$ )

$$\beta A = 2\alpha (\alpha\delta - \beta\gamma) h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g.$$

Точно так же

$$\begin{aligned}\delta A &= a\alpha^2\delta + 2b\alpha\gamma\delta + b\gamma^2\delta = \\ &= \alpha^2\delta^2\gamma + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma^2h = \\ &= (\alpha\delta - \beta\gamma)^2f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f.\end{aligned}$$

Поэтому

$$\alpha = \frac{\beta A - g}{2h}, \quad \gamma = \frac{\delta A - f}{2h}.$$

Если совершенно таким же образом положить

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \quad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g',$$

то

$$\alpha' = \frac{\beta' A - g'}{2h}, \quad \gamma' = \frac{\delta' A - f'}{2h}.$$

Если эти значения  $\alpha, \gamma, \alpha', \gamma'$  подставить в выведенную выше формулу для преобразования формы  $F$  в  $F'$ , то она перейдет в следующую:

$$\frac{\beta f' - \delta' g}{2h}, \quad \frac{\beta' g - \beta g'}{2h}, \quad \frac{\delta f' - \delta' f}{2h}, \quad \frac{\beta' f - \delta g'}{2h},$$

в которой  $A$  уже не содержится.

Если даны две несобственно эквивалентные формы  $F, F'$  и ищется собственное преобразование одной в другую, то пусть  $G$  противоположна форме  $F$  и собственное преобразование формы  $G$  в  $F'$  следующее:  $\alpha, \beta, \gamma, \delta$ . Тогда  $\alpha, \beta, -\gamma, -\delta$ , очевидно, будет несобственным преобразованием формы  $F$  в  $F'$ .

Наконец, ясно, что если заданные формы эквивалентны как собственно, так и несобственно, то тем же способом могут быть найдены два преобразования, одно собственное и одно несобственное.

Итак, остается только показать, как из одного преобразования могут быть выведены все остальные, однотипные с ним. Но это зависит от решения неопределенного уравнения  $t^2 - h^2 u^2 = m^2$ , где  $m$

обозначает наибольший общий делитель чисел  $a$ ,  $2b$  и  $c$ , и  $(a, b, c)$  — одну из двух эквивалентных форм. А это уравнение всегда разрешимо только двумя способами, именно, или посредством  $t = m$ ,  $u = 0$ , или посредством  $t = -m$ ,  $u = 0$ . Действительно, если мы предположим, что существует еще и другое решение  $t = T$ ,  $u = U$ , для которого  $U$  не равно нулю, то будет  $\frac{4T^2}{m^2} = \frac{4U^2h^2}{m^2} + 4$ , и так как  $m^2$  заведомо входит в  $4h^2$ , как  $4T^2/m^2$ , так и  $4h^2U^2/m^2$  будут квадратами целых чисел. Но легко видеть, что число 4 только тогда может быть разностью двух целых квадратов, когда меньший квадрат равен нулю, т. е.  $U = 0$ , что противоречит предположению. Поэтому если форма  $F$  переходит в форму  $F'$  при подстановке  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$ , то, кроме преобразования  $-\alpha$ ,  $-\beta$ ,  $-\gamma$ ,  $-\delta$ , других преобразований, однотипных с ней, не будет. Поэтому если формы эквивалентны только собственно или только несобственно, то имеется лишь два преобразования; если же они эквивалентны как собственно, так и несобственно, то их имеется четыре, именно, два собственных и два несобственных.

## 210

**Теорема.** Если две приведенные формы  $(a, h, 0)$ ,  $(a', h, 0)$  несобственно эквивалентны, то  $aa' \equiv m^2 \pmod{2mh}$ , где  $m$  обозначает наибольший общий делитель чисел  $a$ ,  $2h$  или  $a'$ ,  $2h$ , и обратно, если  $a$ ,  $2h$  и  $a'$ ,  $2h$  имеют один и тот же наибольший общий делитель  $m$ , и  $aa' \equiv m^2 \pmod{2mh}$ , то формы  $(a, h, 0)$ ,  $(a', h, 0)$  несобственно эквивалентны.

**Доказательство.** I Пусть форма  $(a, h, 0)$  переводится в форму  $(a', h, 0)$  не собственной подстановкой  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$ , так что имеют место четыре равенства:

$$[1] \quad a\alpha^2 + 2h\alpha\gamma = a',$$

$$[2] \quad a\alpha\beta + h(\alpha\delta + \beta\gamma) = h,$$

$$[3] \quad a\beta^2 + 2h\beta\delta = 0,$$

$$[4] \quad \alpha\delta - \beta\gamma = -1.$$

Из них следует, если мы умножим [4] на  $h$  и вычтем из [2] (что кратко мы выразим в виде  $[2] - h[4]$ ), что

$$[5] \quad (a\alpha + 2h\gamma)\beta = 2h.$$

Аналогично из  $\gamma\delta[2] - \gamma^2[3] - (a + a\gamma\beta + h\gamma\delta)[4]$ , после того как мы отбросим взаимно уничтожающиеся члены, следует, что

$$[6] \quad -a\alpha\delta = a + 2h\gamma\delta, \text{ или } -(a\alpha + 2h\gamma)\delta = a;$$

наконец, из  $a[1]$  получаем  $a\alpha(a\alpha + 2h\gamma) = aa'$ , или

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma),$$

или

$$[7] \quad (a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)}.$$

Но теперь из [5] и [6] следует, что  $a\alpha + 2h\gamma$  входит в  $2h$  и  $a$ , и потому также и в  $m$ , которое является наибольшим общим делителем  $a$  и  $2h$ ; но очевидно, что  $m$  также будет входить в  $a\alpha + 2h\gamma$ , поэтому обязательно  $a\alpha + 2h\gamma$  равно или  $+m$ , или  $-m$ , а потому из [7] тотчас же следует, что  $m^2 \equiv aa' \pmod{2mh}$ .

II. Если  $a, 2h; a', 2h$  имеют один и тот же наибольший общий делитель  $m$ , и кроме того,  $aa' \equiv m^2 \pmod{2mh}$ , то числа  $a/m, 2h/m, a'/m, (aa' - m^2)/2mh$  будут целыми. Но легко убедиться, что форма  $(a, h, 0)$  переходит в форму  $(a', h, 0)$  при подстановке  $-a'/m, -2h/m, (aa' - m^2)/2mh, a/m$ , и что это преобразование несобственное. Поэтому эти формы несобственно эквивалентны.

Следовательно, мы можем также сразу судить о том, эквивалентна ли несобственно самой себе заданная приведенная форма. Именно, если обозначить наибольший общий делитель чисел  $a, 2h$  через  $m$ , то должно быть  $a^2 \equiv m^2 \pmod{2mh}$ .

Мы получим все приведенные формы с данным определителем  $h^2$ , если в неопределенной форме  $(A, h, 0)$  представим вместо  $A$  все числа от 0 до  $2h - 1$  включительно; количество их тем самым равно  $2h$ . Очевидно, что все формы с определителем  $h^2$  могут быть разбиты на столько же классов, и они будут обладать теми же свойствами,

которые мы получили выше (пп. 175, 195) для классов форм с отрицательным и с положительным неквадратным определителем. Так, например, все формы с определителем 25 распадаются на десять классов, которые могут различаться по содержащимся в каждом из них приведенным формам. Эти приведенные формы суть  $(0, 5, 0)$ ,  $(1, 5, 0)$ ,  $(2, 5, 0)$ ,  $(5, 5, 0)$ ,  $(8, 5, 0)$ ,  $(9, 5, 0)$ , которые одновременно несобственно эквивалентны самим себе;  $(3, 5, 0)$ , которая несобственно эквивалентна форме  $(7, 5, 0)$ , и  $(4, 5, 0)$ , которая несобственно эквивалентна форме  $(6, 5, 0)$ .

## 212

**Задача.** Найти все представления заданного числа  $M$  заданной формой  $ax^2 + 2bxy + cy^2$  с определителем  $h^2$ .

Решение этой задачи могло бы быть получено из соображений п. 168 точно тем же способом, который мы указали выше (пп. 180, 181, 205) для форм с отрицательным и положительным неквадратным определителем; так как это не может вызвать затруднений, было бы излишне повторять здесь то же самое. Однако будет не лишним вывести решение из других соображений, характерных именно для этого случая.

Если, как и в пп. 206, 208, положить

$$(h - b) : a = c : [-(h + b)] = \beta : \delta,$$

$$\frac{h - b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-(h + b)}{\delta} = g.$$

то легко установить, что заданная форма является произведением  $\delta x - \beta y$  и  $fx - gy$ . Отсюда вытекает, что каждое представление числа  $M$  заданной формой дает разложение числа  $M$  на два множителя. Если поэтому  $d, d', d'', \dots$  — всевозможные делители числа  $M$  (куда причисляются также 1 и  $M$ , и каждый отдельный сомножитель учитывается два раза, именно, как положительным, так и отрицательным), то все представления числа  $M$  будут, очевидно, получены, если последовательно положить

$$\delta x - \beta y = d, \quad fx - gy = \frac{M}{d};$$

$$\delta x - \beta y = d', \quad fx - gy = \frac{M}{d'};$$

и т. д., найти отсюда значения  $x$  и  $y$  и выбросить те представления, в которых  $x$  или  $y$  получают дробные значения. Очевидно, кстати, что из двух первых равенств следует, что

$$x = \frac{\beta M - g d^2}{(\beta f - \delta g) d}, \quad y = \frac{\delta M - f d^2}{(\beta f - \delta g) d},$$

а то, что эти значения всегда *определенны*, вытекает из того, что  $\beta f - \delta g = 2h$ , и потому знаменатель заведомо не равен нулю. Между прочим, из этого же принципа, именно, из того, что каждая форма с квадратным определителем может быть разложена на два сомножителя, могут быть решены и остальные проблемы; однако мы предпочитали и здесь использовать метод, аналогичный тому, который мы указали выше для форм с неквадратным определителем.

**Пример.** Найдем все представления числа 12 формой  $3x^2 + 4xy - 7y^2$ . Она распадается на сомножители  $x - y$  и  $3x + 7y$ . Всевозможные делители числа 12 суть  $\pm 1, 2, 3, 4, 6, 12$ . Если положить  $x - y = 1$ ,  $3x + 7y = 12$ , то получается  $x = \frac{19}{10}$ ,  $y = \frac{9}{10}$ ; эти значения, так как они дробны, должны быть выброшены. Точно так же получаются непригодные значения и из делителей  $-1, \pm 3, \pm 4, \pm 6, \pm 12$ . Из делителя же  $+2$  получаются значения  $x = 2, y = 0$ , и из делителя  $-2$  — значения  $x = -2, y = 0$ . Других представлений, кроме этих двух, не существует.

Этот метод неприменим, когда  $M = 0$ . Действительно, в этом случае все значения  $x, y$  должны удовлетворять или уравнению  $\delta x - \beta y = 0$ , или уравнению  $fx - gy = 0$ . Но все решения первого уравнения содержатся в формуле  $x = \beta z, y = \delta z$ , где  $z$  обозначает произвольное целое число (поскольку, как предполагается,  $\beta, \delta$  взаимно просты) и точно так же, если наибольший общий делитель чисел  $f, g$  положить равным  $m$ , то все решения второго уравнения будут представляться формулой  $x = \frac{gz}{m}, y = \frac{fz}{m}$ . Поэтому в этом случае обе эти общие формулы охватывают все представления числа  $M$ .

Теперь все, что относится к вопросу об эквивалентности, к отысканию всех преобразований форм и к получению всех представлений заданного числа заданной формой, мы изложили настолько

полно, что больше желать уже нечего. Поэтому остается только еще показать, как узнать, если заданы две формы, которые не могут быть эквивалентными вследствие того, что не равны их определители, содержится ли одна из них в другой, и если это имеет место, то как найти все преобразования первой во вторую.

### Формы, которые содержатся в других и притом им не эквивалентны

213

Выше, в пп. 157, 158, мы, показали, что если форма  $f$  с определителем  $D$  содержит форму  $F$  с определителем  $E$  и переходит в нее при подстановке  $\alpha, \beta, \gamma, \delta$ , то  $E = (\alpha\delta - \beta\gamma)^2 D$ ; далее, что если  $\alpha\delta - \beta\gamma = \pm 1$ , то форма  $f$  не только содержит форму  $F$ , но и эквивалентна ей, и что вследствие этого если  $f$  только содержит форму  $F$ , но не эквивалентна ей, то отношение  $E/D$  является целым числом, превосходящим единицу. Поэтому здесь нужно решить задачу о том, как *узнать, содержит ли заданная форма  $f$  с определителем  $D$  заданную форму  $F$  с определителем  $De^2$* , причем предполагается, что  $e$  положительное целое число, большее чем 1. Мы решим эту задачу таким образом, что покажем, как может быть найдено конечное число форм, содержащихся в  $f$  и обладающих тем свойством, что если форма  $F$  содержится в  $f$ , то она обязательно должна быть эквивалентна одной из этих форм.

1. Предположим, что все (положительные) делители числа  $e$  (включая 1 и  $e$ ) суть  $m, m', m'', \dots$ , и что  $e = mn = m'n' = m''n'', \dots$ . Для краткости мы будем обозначать форму, в которую  $f$  переходит при собственной подстановке  $m, 0, 0, n$ , через  $(m; 0)$ ; форму, в которую  $f$  переходит при собственной подстановке  $m, 1, 0, n$ , через  $(m; 1)$  и т. д., вообще, форму, в которую  $f$  переходит при собственной подстановке  $m, k, 0, n$ , через  $(m; k)$ . Аналогично, пусть  $f$  при собственной подстановке  $m', 0, 0, n'$  переходит в  $(m'; 0)$ , при подстановке  $m', 1, 0, n'$  — в  $(m'; 1)$ , и т. д., при подстановке  $m'', 0, 0, n''$ , — в  $(m''; 0)$  и т. д., и т. д. Все эти формы собственно содержатся в  $f$ , и определитель каждой из них равен  $De^2$ . Совокупность

всех форм  $(m; 0), (m; 1), (m; 2), \dots, (m; m-1); (m'; 0), (m'; 1), \dots, (m'; m'-1); (m''; 0), \dots$ , число которых равно  $m + m' + m'' + \dots$ , и которые, как легко видеть, все между собой различны, мы обозначим через  $\Omega$ .

Если, например,  $f$  есть форма  $(2, 5, 7)$  и  $e = 5$ , то  $\Omega$  будет охватывать следующие шесть форм:  $(1; 0), (5; 0), (5; 1), (5; 2), (5; 3), (5; 4)$ , — которые в развернутом виде имеют вид  $(2, 25, 175), (50, 25, 7), (50, 35, 19), (50, 45, 35), (50, 55, 55), (50, 65, 79)$ .

II. Я утверждаю теперь, что если форма  $F$  с определителем  $De^2$  собственно содержится в  $f$ , то она обязательно собственно эквивалентна какой-нибудь форме из  $\Omega$ . Действительно, если  $f$  переходит в  $F$  при собственной подстановке  $\alpha, \beta, \gamma, \delta$ , то  $\alpha\delta - \beta\gamma = e$ . Пусть, далее, наибольший общий (взятый положительным) делитель чисел  $\gamma, \delta$  (которые не могут быть оба равны 0) равен  $n$  и  $\frac{e}{n} = m$ , причем это число, очевидно, целое. Предположим  $g, h$  такими, что  $\gamma g + \delta h = n$ , и, наконец, пусть  $k$  — наименьший положительный вычет числа  $\alpha g + \beta h$  по модулю  $m$ . Тогда форма  $(m; k)$ , которая, очевидно, содержится среди форм  $\Omega$ , будет собственно эквивалентна форме  $F$ , причем первая переходит во вторую при собственной подстановке

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}.$$

Действительно, прежде всего ясно, что все эти четыре числа целые; точно так же легко устанавливается, что подстановка собственная; наконец, очевидно, что форма, в которую переходит при этой подстановке  $(m; k)$ , будет та же самая, в которую переходит  $f^*$  при подстановке

$$m \left( \frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h \right) + \frac{k\gamma}{n}, \quad m \left( \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g \right) + \frac{k\delta}{n}, \quad \gamma, \delta$$

или, так как  $mn = e = \alpha\delta - \beta\gamma$ , и потому  $\beta\gamma + mn = \alpha\delta$ ,  $\alpha\delta - mn = \beta\gamma$ , при подстановке

$$\frac{1}{n} (\alpha\gamma g + \alpha\delta h), \quad \frac{1}{n} (\beta\gamma g + \beta\delta h), \quad \gamma, \delta,$$

\* Которая при подстановке  $m, k, 0, n$  переходит в  $(m; k)$  (ср. п. 159).



или, наконец, в силу  $\gamma g + \delta h = n$ , при подстановке  $\alpha, \beta, \gamma, \delta$ , т. е., согласно предположению, в  $F$ . Поэтому формы  $(m; k)$  и  $F$  собственно эквивалентны.

Таким образом всегда можно узнать, содержит ли собственно заданная форма  $f$  с определителем  $D$  форму  $F$  с определителем  $De^2$ . Если же спрашивается, содержит ли  $f$  форму  $F$  несобственно, то нужно только исследовать, содержится ли собственно в  $f$  форма противоположная  $F$  (п. 159).

## 214

**Задача.** Пусть даны две формы,  $f$  с определителем  $D$  и  $F$  с определителем  $De^2$ , первая из которых собственно содержит вторую; требуется представить все собственные преобразования формы  $f$  в  $F$ .

**Решение.** Если  $\Omega$  обозначает ту же совокупность форм, что в предыдущем пункте, то нужно выбрать из этой совокупности все формы, которым  $F$  собственно эквивалентна; пусть это формы  $\Phi, \Phi', \Phi'', \dots$ . Каждая из этих форм дает излагаемым ниже способом собственные преобразования формы  $f$  в  $F$ , причем отдельные формы дают различные преобразования, а все вместе — всевозможные преобразования (т. е. не существует собственного преобразования формы  $f$  в  $F$ , которое не получалось бы из одной из форм  $\Phi, \Phi', \dots$ ). Так как метод для всех форм  $\Phi, \Phi', \dots$  одинаков, мы будем говорить только об одной из них.

Предположим, что  $\Phi = (M; K)$  и  $e = MN$ , так что  $f$  переходит в  $\Phi$  при собственной подстановке  $M, K, 0, N$ . Далее, произвольное собственное преобразование формы  $\Phi$  в  $F$  мы обозначим через  $a, b, c, d$ . Тогда  $f$  будет, очевидно, переходить в  $\Phi$  при собственной подстановке  $Ma + Kc, Mb + Kd, Nc, Nd$ , и этим способом из каждого собственного преобразования формы  $\Phi$  в  $F$  получается собственное преобразование формы  $f$  в  $F$ . Таким же образом можно поступать и с остальными формами  $\Phi', \Phi'', \dots$ , отдельные собственные преобразования которых в  $F$  дают собственные преобразования формы  $f$  в  $F$ .

Чтобы сделать ясным, что это решение во всех отношениях является исчерпывающим, нужно показать следующее.

I. Что при этом получают все возможные собственные преобразования формы  $f$  в  $F$ . Пусть  $\alpha, \beta, \gamma, \delta$  — какое-нибудь собственное преобразование формы  $f$  в  $F$ , и, как и в предложении II предыдущего пункта,  $n$  — наибольший общий делитель чисел  $\gamma, \delta$ ; числа же  $m, g, h, k$  пусть определены таким же образом, как и там. Тогда  $(m; k)$  будет находиться среди форм  $\Phi, \Phi', \dots$ , и

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

будет собственным преобразованием этой формы в  $F$ ; а из него мы по указанному выше правилу получаем преобразование  $\alpha, \beta, \gamma, \delta$ . Все это было доказано в предыдущем пункте.

II. Что все получающиеся таким образом преобразования различны, т. е. что ни одно не получается дважды. При этом мы убеждаемся без труда, что несколько различных преобразований одной и той же формы  $\Phi$ , или  $\Phi'$ , и т. д. в  $F$  не может дать одно и то же преобразование формы  $f$  в  $F$ ; а то, что и различные формы, например,  $\Phi$  и  $\Phi'$ , не дают одного и того же преобразования, доказывается так. Предположим, что собственное преобразование  $\alpha, \beta, \gamma, \delta$  формы  $f$  в  $F$  получается как из собственного преобразования  $a, b, c, d$  формы  $\Phi$  в  $F$ , так и из собственного преобразования  $a', b', c', d'$  формы  $\Phi'$  в  $F$ . Далее, пусть  $\Phi = (M; K)$ ,  $\Phi' = (M'; K')$ ;  $e = MN = M'N'$ . Тогда имеют место равенства:

$$[1] \quad \alpha = Ma + Kc = M'a' + K'c',$$

$$[2] \quad \beta = Mb + Kd = M'b' + K'd',$$

$$[3] \quad \gamma = Nc = N'c',$$

$$[4] \quad \delta = Nd = N'd',$$

$$[5] \quad ad - bc = a'd' - b'c' = 1.$$

Из  $a$  [4] —  $b$  [3] при помощи равенства [5] получаем, что  $N = N' \times \times (ad' - bc')$ , поэтому  $N'$  входит в  $N$ ; аналогично, из  $a'$  [4] —  $b'$  [3] следует, что  $N(a'd - b'c) = N'$ , и потому  $N$  входит в  $N'$ ; следовательно, так как и  $N$  и  $N'$  предполагаются положительными, обязательно  $N = N'$  и  $M = M'$ , и значит, в силу [3] и [4],  $c = c'$ ,  $d = d'$ . Далее, из  $a$  [2] —  $b$  [1] следует, что

$$K = M'(ab' - ba') + K'(ad' - bc') = M(ab' - ba') + K';$$

тем самым  $K \equiv K' \pmod{M}$ , а это возможно только в том случае, если  $K = K'$ , потому что как  $K$ , так и  $K'$  лежат между границами 0 и  $M - 1$ . Поэтому формы, вопреки предположению, не являются различными.

Ясно, что если  $D$  отрицательно или является положительным квадратом, то этим методом действительно могут быть найдены все собственные преобразования формы  $f$  в  $F$ ; если же число  $D$  положительно, но не является квадратом, то могут быть даны некоторые общие формулы, в которых содержатся все собственные преобразования (число которых бесконечно велико).

Наконец, если форма  $F$  содержится в форме  $f$  несобственно, то все несобственные преобразования первой во вторую легко могут быть получены указанным методом. Именно, если  $\alpha, \beta, \gamma, \delta$  пробегает все собственные преобразования формы  $f$  в форму, противоположную форме  $F$ , то все возможные несобственные преобразования формы  $f$  в  $F$  представляются в виде  $\alpha, -\beta, \gamma, -\delta$ .

**Пример.** Требуется найти все преобразования формы  $(2, 5, 7)$  в форму  $(275, 0, -1)$ , которая содержится в первой как собственно, так и несобственно. Совокупность форм  $\Omega$  для этого случая мы указали уже в предыдущем пункте; исследование дает, что как  $(5; 1)$ , так и  $(5; 4)$  собственно эквивалентны форме  $(275, 0, -1)$ . В соответствии с изложенной выше теорией находим, что всевозможные собственные преобразования формы  $(5; 1)$ , т. е. формы  $(50, 35, 19)$ , в форму  $(275, 0, -1)$  содержатся в общей формуле

$$16t - 275u, -t + 16u, -15t + 275u, t - 15u,$$

где  $t, u$  обозначают всевозможные целые числа, удовлетворяющие уравнению  $t^2 - 275u^2 = 1$ . Поэтому все получающиеся отсюда собственные преобразования формы  $(2, 5, 7)$  в форму  $(275, 0, -1)$  будут содержаться в общей формуле

$$65t - 1100u, -4t + 65u, -15t + 275u, t - 15u.$$

Аналогичным образом всевозможные собственные преобразования формы  $(5; 4)$ , т. е. формы  $(50, 65, 79)$ , в форму  $(275, 0, -1)$  содержатся в общей формуле

$$14t + 275u, t + 14u, -15t - 275u, -t - 15u,$$

и потому все собственные преобразования формы (2, 5, 7) в форму (275, 0, —1), которые отсюда получаются,— в формуле

$$10t + 275u, \quad t + 10u, \quad -15t - 275u, \quad -t - 15u.$$

Обе эти формулы охватывают, таким образом, все искомые собственные преобразования\*. Подобным же образом находим, что все возможные несобственные преобразования формы (2, 5, 7) в форму (275, 0, —1) содержатся в следующих двух формулах:

$$\begin{aligned} 65t - 1100u, \quad 4t - 65u, \quad -15t + 275u, \quad -t + 15u; \\ 10t + 275u, \quad -t - 10u, \quad -15t - 275u, \quad t + 15u. \end{aligned}$$

### Формы с определителем 0

215

До сих пор формы с определителем 0 мы из всех рассмотренных исключали; поэтому, чтобы сделать нашу теорию исчерпывающей во всех отношениях, мы должны еще добавить кое-что и о них. Доказано вообще, что если какая-нибудь форма с определителем  $D$  содержит форму с определителем  $D'$ , то  $D'$  является кратностью  $D$ ; поэтому ясно, что форма, определитель которой равен 0, не может содержать никаких других форм, кроме тех, у которых определитель тоже равен 0. Таким образом остается решить *только две задачи*, именно: 1) Пусть даны две формы  $f, F$ , вторая из которых имеет определитель 0; требуется узнать, содержит ли первая форма вторую, или нет, и в первом случае представить все преобразования первой формы во вторую; 2) найти все представления заданного числа заданной формой с определителем 0.

Первая задача требует различных методов, когда определитель первой формы  $f$  тоже равен 0, и когда он не равен 0. Все это мы теперь и изложим.

I. Прежде всего заметим, что каждая форма  $ax^2 + 2bxy + cy^2$ , определитель которой  $b^2 - ac = 0$ , может быть представлена в виде

---

\* Короче все собственные преобразования представляются формулой

$$10t + 55u, \quad t + 2u, \quad -15t - 55u, \quad -t - 3u,$$

где  $t, u$  пробегают все числа, удовлетворяющие уравнению  $t^2 - 11u^2 = 1$ .

$m(gx + hy)^2$ , где  $g$  и  $h$  обозначают взаимно простые числа, а  $m$  — целое число. Именно, если  $m$  — наибольший общий делитель чисел  $a$ ,  $c$ , причем взятый с тем же знаком, который имеют сами эти числа (легко видеть, что эти числа не могут иметь противоположных знаков), то  $a/m$ ,  $c/m$  будут целыми взаимно простыми неотрицательными числами, а их произведение равно  $b^2/m^2$ , т. е. является квадратом, а потому и сами они тоже квадраты (п. 21).

Если  $\frac{a}{m} = g^2$ ,  $\frac{c}{m} = h^2$ , то  $g$  и  $h$  также взаимно просты, далее,  $g^2 h^2 = \frac{b^2}{m^2}$  и  $gh = \pm \frac{b}{m}$ . Отсюда вытекает, что

$$m(gx \pm hy)^2 = ax^2 + 2bxy + cy^2.$$

Пусть теперь даны две формы  $f$ ,  $F$  с определителем 0, причем пусть

$$f = m(gx + hy)^2, \quad F = M(GX + HY)^2,$$

так что  $g$  взаимно просто с  $h$ , и  $G$  — с  $H$ . Тогда я утверждаю, что если форма  $f$  содержит форму  $F$ , то  $m$  или равно  $M$ , или по меньшей мере входит в  $M$ , причем отношение тогда является квадратом, и обратно, если  $M/m$  есть целочисленный квадрат, то  $F$  содержится в  $f$ . Именно, если предположить, что  $f$  переходит в  $F$  при подстановке

$$x = \alpha X + \beta Y, \quad y = \gamma X + \delta Y,$$

то

$$\frac{M}{m} (GX + HY)^2 = [(\alpha g + \gamma h) X + (\beta g + \delta h) Y]^2,$$

откуда легко следует, что  $M/m$  есть квадрат. Если положить его равным  $e^2$ , то

$$e(GX + HY) = \pm [(\alpha g + \gamma h) X + (\beta g + \delta h) Y],$$

т. е.

$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h.$$

Если поэтому  $\mathfrak{G}$ ,  $\mathfrak{H}$  определены так, что  $\mathfrak{G}G + \mathfrak{H}H = \pm 1$ , то

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h) = \text{целому числу}.$$

Если же, наоборот, предположить, что  $M/t$  является целым квадратом и равно  $e^2$ , то форма  $f$  будет содержать форму  $F$ . Именно, можно будет так определить целые числа  $\alpha, \beta, \gamma, \delta$ , что

$$\alpha g + \gamma h = \pm eG, \quad \beta g + \delta h = \pm eH.$$

Действительно, если целые числа  $g, h$  выбраны так, что  $g^2 + h^2 = 1$ , то указанные равенства будут выполняться, если положить

$$\begin{aligned} \alpha &= \pm eGg + hz, & \gamma &= \pm eGh - gz, \\ \beta &= \pm eHg + hz', & \delta &= \pm eHh - gz', \end{aligned}$$

где  $z$  и  $z'$  могут иметь любые целочисленные значения. Поэтому  $F$  будет содержаться в  $f$ . Одновременно можно без труда убедиться, что эти формулы представляют все значения, которые могут принимать  $\alpha, \beta, \gamma, \delta$ , т. е. все преобразования формы  $f$  в  $F$ , если, только предположить, что  $z$  и  $z'$  пробегает все целые числа.

II. Если даны две формы,  $f = ax^2 + 2bxy + cy^2$ , определитель которой не равен 0, и  $F = M(GX + HY)^2$ , определитель которой равен 0, то я утверждаю, во-первых, что если  $f$  содержит форму  $F$ , то число  $M$  может быть представлено формой  $f$ ; во-вторых, что если  $M$  может быть представлено формой  $f$ , то  $F$  содержится в  $f$ ; в-третьих, что если в этом случае произвольное представление числа  $M$  формой  $f$  есть  $x = \xi, y = \upsilon$ , то  $G\xi, H\xi, G\upsilon, H\upsilon$  будет пробегать все преобразования формы  $f$  в  $F$ . Все это мы докажем следующим образом.

1. Если предположим, что  $f$  переходит в  $F$  при подстановке  $\alpha, \beta, \gamma, \delta$ , и определим числа  $\mathfrak{G}, \mathfrak{H}$  так, что  $\mathfrak{G}G + \mathfrak{H}H = 1$ , то если положить  $x = \alpha\mathfrak{G} + \beta\mathfrak{H}, y = \gamma\mathfrak{G} + \delta\mathfrak{H}$ , значение формы  $f$  будет, очевидно, равно  $M$ , и потому  $M$  представляется формой  $f$ .

2. Если предположить, что  $a\xi^2 + 2b\xi\upsilon + c\upsilon^2 = M$ , то при подстановке  $G\xi, H\xi, G\upsilon, H\upsilon$  форма  $f$ , очевидно, переходит в  $F$ .

3. То, что в этом случае подстановки  $G\xi, H\xi, G\upsilon, H\upsilon$  дают все преобразования формы  $f$  в  $F$ , если предположить, что  $\xi, \upsilon$  пробегает все значения  $x, y$ , при которых  $f = M$ , показывается так. Если  $\alpha, \beta, \gamma, \delta$  — какое-нибудь преобразование формы  $f$  в  $F$ , и, как и раньше,  $\mathfrak{G}G + \mathfrak{H}H = 1$ , то среди значений  $x, y$  будут находиться также и следующие:

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H} \quad y = \gamma\mathfrak{G} + \delta\mathfrak{H},$$

а из них мы получаем подстановку

$$G(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad H(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad G(\gamma\mathfrak{G} + \delta\mathfrak{H}), \quad H(\gamma\mathfrak{G} + \delta\mathfrak{H}),$$

или

$$\alpha + \mathfrak{H}(\beta G - \alpha H), \quad \beta + \mathfrak{G}(\alpha H - \beta G),$$

$$\gamma + \mathfrak{H}(\delta G - \gamma H), \quad \delta + \mathfrak{G}(\gamma H - \delta G).$$

Так как, однако,

$$\begin{aligned} a(\alpha X + \beta Y)^2 + 2b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 = \\ = M(GX + HY)^2, \end{aligned}$$

то

$$a(\alpha\delta - \beta\gamma)^2 = M(\delta G - \gamma H)^2,$$

$$c(\beta\gamma - \alpha\delta)^2 = M(\beta G - \alpha H)^2,$$

и потому (так как определитель формы  $f$ , умноженный на  $(\alpha\delta - \beta\gamma)^2$ , равен определителю формы  $F$ , т. е. равен 0, и потому  $\alpha\delta - \beta\gamma = 0$ )

$$\delta G - \gamma H = 0, \quad \beta G - \alpha H = 0.$$

Поэтому наша подстановка переходит в  $\alpha, \beta, \gamma, \delta$ , откуда вытекает, что указанная формула дает все преобразования формы  $f$  в  $F$ .

III. Нам остается еще только показать, как можно найти все представления заданного числа заданной формой с определителем 0. Если заданная форма есть  $m(gx + hy)^2$ , то тотчас же ясно, что число должно делиться на  $m$ , и отношение должно быть квадратом. Если поэтому положить заданное число равным  $me^2$ , то очевидно, что для тех значений  $x, y$ , для которых  $m(gx + hy)^2 = me^2$ ,  $gx + hy$  должно быть равно или  $+e$ , или  $-e$ . Поэтому мы получим все представления, если найдем все решения линейных уравнений  $gx + hy = e$  и  $gx + hy = -e$  в целых числах. То, что они разрешимы, известно (если, как и предполагается,  $g$  и  $h$  взаимно просты). Именно, если  $g, h$  определены так, что  $gg + hh = 1$ , то первое уравнение будет удовлетворяться, если положить  $x = ge + hz$ ,  $y = he - gz$ , а второе, — если положить  $x = -ge + hz$ ,  $y = -he - gz$ , где  $z$  обозначает какое-нибудь целое число. Одновременно эти формулы будут давать все целочисленные значения  $x, y$ , если считать, что  $z$  пробегает все целые числа.

## Общее решение в целых числах всех неопределенных уравнений второй степени с двумя неизвестными

216

В качестве заключения этих исследований, мы добавим еще одну задачу.

**Задача.** Найти все решения в целых числах общего неопределенного уравнения второй степени с двумя неизвестными:

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0^*$$

(где  $a, b, c, \dots$  — любые заданные целые числа).

**Решение.** Мы введем вместо неизвестных  $x, y$  другие:

$$p = (b^2 - ac)x + be - cd, \quad q = (b^2 - ac)y + bd - ae,$$

которые, очевидно, всегда будут целыми числами, если  $x$  и  $y$  целые. Тогда мы получим уравнение

$$ap^2 + 2bpq + cq^2 + f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = 0,$$

или, если для краткости положить

$$f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = -M,$$

то

$$ap^2 + 2bpq + cq^2 = M.$$

Но раньше мы показали, как могут быть найдены все решения этого уравнения, т. е. все представления числа  $M$  формой  $(a, b, c)$ . Если же из отдельных пар значений  $p, q$  определить соответствующие значения  $x, y$  при помощи равенств

$$x = \frac{p + cd - be}{b^2 - ac}, \quad y = \frac{q + ae - bd}{b^2 - ac},$$

то легко видеть, что все эти значения удовлетворяют заданному уравнению, и не существует целочисленных значений  $x, y$ , которые не получались бы таким способом. Если мы, поэтому, из всех так

---

\* Если бы было дано некоторое уравнение, у которого был бы нечетным второй, четвертый или пятый коэффициент, то после умножения на 2 оно привелось бы к виду, предполагаемому здесь.



получающихся значений  $x, y$  выбросим дробные значения, то останутся все искомые решения.

*Относительно этого решения нужно сделать следующие замечания.*

1. Если либо число  $M$  не может быть представлено формой  $(a, b, c)$ , либо ни из какого его представления не получается целых значений  $x, y$ , то уравнение не может быть разрешимо в целых числах.

2. Если определитель формы  $(a, b, c)$ , т. е. число  $b^2 - ac$ , отрицателен, или же положителен, является квадратом и одновременно  $M$  не равно 0, то количество представлений числа  $M$  формой  $(a, b, c)$  будет конечным, и тем самым будет конечным и количество решений (если они вообще существуют) заданного уравнения.

3. Если  $b^2 - ac$  — положительное число, не являющееся квадратом, или же квадрат, но одновременно  $M = 0$ , то если число  $M$  вообще может быть представлено формой  $(a, b, c)$  хотя бы одним способом, оно будет представляться *бесконечным количеством способов*; так как, однако, невозможно найти все эти представления и исследовать, дают ли они целые значения  $x, y$  или дробные, то необходимо указать метод, при помощи которого в случае, когда ни одно представление не дает целых значений  $x, y$ , можно в этом удостовериться (действительно, мы покажем, сколько в этом случае надо исследовать представлений, в чем ведь никогда нельзя было бы быть уверенным без такого правила); если же одни представления дают целые, а другие — дробные значения  $x, y$ , то нужно будет показать, как вообще сразу можно отличать первые от вторых.

4. Если  $b^2 - ac = 0$ , то значения  $x, y$  вообще не могут быть определены по указанным выше формулам; поэтому в этом случае нужно сообщить специальный способ.

Для случая, когда  $b^2 - ac$  — *положительное число, не являющееся квадратом*, мы выше показали, что всевозможные представления числа  $M$  формой  $ar^2 + 2brq + cq^2$  (если они вообще существуют)

могут быть определены по одной или нескольким формулам вида

$$p = \frac{1}{m} (\mathfrak{A}t + \mathfrak{B}u), \quad q = \frac{1}{m} (\mathfrak{C}t + \mathfrak{D}u),$$

где  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$  — заданные целые числа,  $m$  — наибольший общий делитель чисел  $a, 2b, c$ , и наконец,  $t, u$  обозначают всевозможные целые числа, удовлетворяющие уравнению  $t^2 - (b^2 - ac)u^2 = m^2$ . Так как значения  $t, u$  можно предполагать как положительными, так и отрицательными, то вместо каждой отдельной из этих формул мы можем получить четыре других:

$$\begin{aligned} p &= \frac{1}{m} (\mathfrak{A}t + \mathfrak{B}u), & q &= \frac{1}{m} (\mathfrak{C}t + \mathfrak{D}u), \\ p &= \frac{1}{m} (\mathfrak{A}t - \mathfrak{B}u), & q &= \frac{1}{m} (\mathfrak{C}t - \mathfrak{D}u), \\ p &= \frac{1}{m} (-\mathfrak{A}t + \mathfrak{B}u), & q &= \frac{1}{m} (-\mathfrak{C}t + \mathfrak{D}u), \\ p &= -\frac{1}{m} (\mathfrak{A}t + \mathfrak{B}u), & q &= -\frac{1}{m} (\mathfrak{C}t + \mathfrak{D}u), \end{aligned}$$

так что количество всех формул теперь вчетверо больше, чем до этого, а  $t$  и  $u$  выражают уже не все числа, удовлетворяющие уравнению  $t^2 - (b^2 - ac)u^2 = m^2$ , а лишь положительные числа такого рода. Каждую из этих формул надо рассмотреть отдельно и исследовать, какие значения  $t, u$  дают целые значения  $x, y$ .

Из выражений

$$[1] \quad p = \frac{1}{m} (\mathfrak{A}t + \mathfrak{B}u), \quad q = \frac{1}{m} (\mathfrak{C}t + \mathfrak{D}u)$$

получаются следующие значения  $x, y$ :

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(b^2 - ac)}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(b^2 - ac)}.$$

Но выше мы показали, что все (положительные) значения  $t$  образуют рекуррентный ряд  $t^0, t', t'', \dots$ , и точно так же соответствующие значения  $u$  образуют рекуррентный ряд  $u^0, u', u'', \dots$ ; что, далее, может быть указано число  $\rho$  с тем свойством, что по некоторому заданному модулю

$$t^{(\rho)} \equiv t^0, \quad t^{(\rho+1)} \equiv t', \quad t^{(\rho+2)} \equiv t'', \dots, \quad u^{(\rho)} \equiv u^0, \quad u^{(\rho+1)} \equiv u', \dots$$

Возьмем за этот модуль число  $m(b^2 - ac)$ , и обозначим для краткости значения  $x, y$ , которые получаются, если положить  $t = t^0$ ,  $u = u^0$  — и которые мы снабдим индексом 0 — через  $x^0, y^0$ ; точно так же те, которые получаются, если положить  $t = t'$ ,  $u = u'$  — и которые мы снабдим индексом 1 — через  $x', y'$ , и т. д. Тогда без труда видно, что если числа  $x^{(h)}, y^{(h)}$  целые и  $\rho$  определено правильно, то и  $x^{(h+\rho)}, y^{(h+\rho)}, x^{(h+2\rho)}, y^{(h+2\rho)}$  и вообще  $x^{(h+k\rho)}, y^{(h+k\rho)}$  будут целыми числами, и что, наоборот, если  $x^{(h)}$  или  $y^{(h)}$  дробно, то и  $x^{(h+k\rho)}$  или  $y^{(h+k\rho)}$  является дробным числом. Отсюда легко выводится, что если найдены значения  $x, y$ , снабженные индексами  $0, 1, 2, \dots, \rho - 1$ , и для каждого из этих индексов или  $x$ , или  $y$  не является целым числом, то вообще нет индекса, для которого как  $x$ , так и  $y$  принимали бы целые значения, так что в этом случае из формулы [1] не могут быть получены целые значения  $x, y$ . Если же среди этих индексов имеются какие-нибудь, скажем  $\mu, \mu', \mu'', \dots$ , которым соответствуют целые значения  $x, y$ , то всеми целыми значениями  $x, y$ , которые могут быть получены из формулы [1], будут те, индексы которых имеют вид  $\mu + k\rho$ , или  $\mu' + k\rho$ , или  $\mu'' + k\rho, \dots$ , где  $k$  пробегает все целые положительные числа, не исключая и нуля.

Остальные формулы, в которых содержатся значения  $p, q$ , разбираются точно таким же способом. В том случае, когда ни из одной из всех этих формул не получаются целые значения  $x, y$ , заданное уравнение само вообще не может быть решено в целых числах; если же оно в действительности разрешимо, то все целочисленные решения могут быть представлены по изложенным выше правилам.

Если  $b^2 - ac$  является квадратом и  $M = 0$ , то все значения  $p, q$  содержатся в двух формулах вида  $p = \mathfrak{A}z, q = \mathfrak{B}z; p = \mathfrak{A}'z, q = \mathfrak{B}'z$ , где  $z$  обозначает произвольное целое число, а  $\mathfrak{A}, \mathfrak{B}, \mathfrak{A}', \mathfrak{B}'$  суть заданные целые числа, первое из которых не имеет общих делителей со вторым, а третье — с четвертым (п. 212). Поэтому все

целочисленные значения  $x, y$ , получающиеся из первой формулы, содержатся в формуле

$$[1] \quad x = \frac{\mathfrak{A}z + cd - be}{b^2 - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{b^2 - ac},$$

а все остальные, получающиеся из второй формулы,— в формуле

$$[2] \quad x = \frac{\mathfrak{A}'z + cd - be}{b^2 - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{b^2 - ac}.$$

Так как, однако, каждая из этих формул может давать также и дробные значения (поскольку не обязательно  $b^2 - ac = 1$ ), мы должны в каждой из этих формул отделить те значения  $z$ , для которых как  $x$ , так и  $y$  будут целыми числами, от остальных; впрочем, достаточно рассмотреть только первую формулу, так как для второй применим в точности тот же метод.

Так как  $\mathfrak{A}, \mathfrak{B}$  взаимно просты, можно найти два такие числа  $\mathfrak{a}, \mathfrak{b}$ , что  $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$ . Если это сделано, то мы имеем

$$(\mathfrak{a}x + \mathfrak{b}y)(b^2 - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd),$$

откуда тотчас же вытекает, что все значения  $z$ , которые могут дать целые значения  $x, y$ , обязательно должны быть сравнимы с числом  $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$  по модулю  $b^2 - ac$ , т. е. содержаться в формуле  $(b^2 - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ , где  $z'$  обозначает произвольное целое число. Поэтому вместо формулы [1] мы легко получаем формулу

$$x = \mathfrak{A}z' + \mathfrak{b} \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{b^2 - ac},$$

$$y = \mathfrak{B}z' - \mathfrak{a} \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{b^2 - ac},$$

которая, очевидно, дает целые значения  $x, y$  или для всех значений  $z'$ , или для никаких, причем первый случай будет иметь место, если  $\mathfrak{A}(bd - ae)$  и  $\mathfrak{B}(be - cd)$  по модулю  $b^2 - ac$  сравнимы, а второй,— если не сравнимы. Точно таким же образом исследуется формула [2], и целочисленные решения (если они этой формулой даются) отделяются от остальных.

Если  $b^2 - ac = 0$ , то форма  $ax^2 + 2bxy + cy^2$  может быть представлена в виде  $m(\alpha x + \beta y)^2$ , где  $m, \alpha, \beta$  являются целыми числами (п. 215). Если положить  $\alpha x + \beta y = z$ , то заданное уравнение переходит в

$$mz^2 + 2dx + 2ey + f = 0,$$

и отсюда в соединении с  $\alpha x + \beta y = z$  следует, что

$$x = \frac{\beta mz^2 + 2ez + \beta f}{2\alpha e - 2\beta d}, \quad y = \frac{\alpha mz^2 + 2dz + \alpha f}{2\beta d - 2\alpha e}.$$

Теперь ясно, что если не имеет места  $\alpha e = \beta d$  (каковой случай мы тотчас же рассмотрим отдельно), то получающиеся из этих формул при любом значении  $z$  значения  $x, y$  удовлетворяют заданному уравнению; поэтому остается только еще показать, как определяются те значения  $z$ , из которых получаются целые значения  $x, y$ .

Так как  $\alpha x + \beta y = z$ , то для  $z$  можно брать только целочисленные значения; кроме того, ясно, что если для некоторого значения  $z$  как  $x$  так и  $y$  будут целыми числами, то и все значения  $z$ , которые сравнимы с ним по модулю  $2\alpha e - 2\beta d$ , тоже будут давать целые значения. Если поэтому подставить вместо  $z$  все целые числа от 0 до  $2\alpha e - 2\beta d - 1$  (в случае, когда  $\alpha e - \beta d$  положительно) или до  $2\beta d - 2\alpha e - 1$  (если  $\alpha e - \beta d$  отрицательно) включительно, и ни для какого из этих значений  $x$  и  $y$  не будут целыми числами, то вообще никакое значение  $z$  не будет давать целочисленных значений  $x, y$ , и заданное уравнение будет вообще неразрешимо в целых числах. Если же некоторые из значений  $z$ , например,  $\zeta, \zeta', \zeta'', \dots$  (которые можно также найти решением сравнений второй степени по правилам раздела IV), дают для  $x, y$  целочисленные значения, то все решения получаются, если положить  $z = (2\alpha e - 2\beta d)v + \zeta$ ,  $z = (2\alpha e - 2\beta d)v + \zeta', \dots$ , где  $v$  пробегает все целые числа.

Для исключенного случая, когда  $\alpha e = \beta d$ , мы должны применить специальный способ. Если мы предположим, что  $\alpha, \beta$  взаимно просты, что, как известно из п. 215, I, позволительно, то  $\frac{d}{\alpha} = \frac{e}{\beta}$  будет целым числом (п. 19), которое мы положим равным  $h$ . Тогда заданное уравнение принимает вид

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf = 0$$

и потому, очевидно, может быть разрешено рационально только в том случае, если  $h^2 - mf$  является квадратом. Если  $h^2 - mf = k^2$ , то ясно, что заданному уравнению эквивалентны оба следующие уравнения:

$$m\alpha x + m\beta y + h + k = 0 \text{ и } m\alpha x + m\beta y + h - k = 0,$$

т. е. что каждое решение заданного уравнения удовлетворяет также тому или другому из этих уравнений, и обратно. Первое уравнение, очевидно, может быть решено в целых числах только тогда, когда  $h + k$  делится на  $m$ ; аналогично, второе уравнение только тогда обладает решением в целых числах, когда  $h - k$  делится на  $m$ . Но эти условия также и достаточны для разрешимости каждого из этих уравнений (так как, по предположению,  $\alpha$  и  $\beta$  взаимно просты), и все их решения могут быть найдены по известным правилам.

Рассмотренный в п. 217 случай (самый трудный из всех) мы поясним примером. Пусть задано уравнение

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0.$$

Сначала посредством введения новых неизвестных

$$p = 15x - 9, \quad q = 15y + 6$$

мы получаем из него уравнение

$$p^2 + 8pq + q^2 = -540.$$

Далее, находим, что все целочисленные решения этого уравнения содержатся в следующих четырех формулах:

$$\begin{aligned} p &= 6t, & q &= -24t - 90u, \\ p &= 6t, & q &= -24t + 90u, \\ p &= -6t, & q &= 24t - 90u, \\ p &= -6t, & q &= 24t + 90, \end{aligned}$$

где  $t, u$  обозначают всевозможные целые положительные числа, которые удовлетворяют уравнению  $t^2 - 15u^2 = 1$  и содержатся в формулах

$$\begin{aligned} t &= \frac{1}{2} [(4 + \sqrt{15})^n + (4 - \sqrt{15})^n], \\ u &= \frac{1}{2\sqrt{15}} [(4 + \sqrt{15})^n - (4 - \sqrt{15})^n], \end{aligned}$$

где  $n$  обозначает всевозможные целые положительные числа (включая и нуль). Поэтому все значения  $x, y$  содержатся в формулах

$$\begin{aligned} x &= \frac{1}{5} (2t + 3), & y &= -\frac{1}{5} (8t + 30u + 2), \\ x &= \frac{1}{5} (2t + 3), & y &= -\frac{1}{5} (8t - 30u + 2), \\ x &= \frac{1}{5} (-2t + 3), & y &= \frac{1}{5} (8t - 30u - 2), \\ x &= \frac{1}{5} (-2t + 3), & y &= \frac{1}{5} (8t + 30u - 2). \end{aligned}$$

Применяя предписанные нами правила, найдем, что для того, чтобы получились *целочисленные* значения, в первой и второй формулах нужно брать те значения  $t, u$ , которые получаются при *четных* показателях  $n$ , а в третьей и четвертой — при *нечетных*  $n$ . В качестве простейших решений мы получаем  $x = 1, -1, -1$ , соответственно  $y = -2, 0, 12$ .

Впрочем, нужно заметить, что решение рассмотренной в предыдущем пункте проблемы в большинстве случаев может быть сокращено посредством многочисленных искусственных приемов, в особенности в отношении непригодных, т. е. содержащих дроби, решений. Однако, чтобы изложение не было слишком пространным, мы предпочитаем здесь это опустить.

## Исторические замечания

222

Так как многое из того, что мы до сих пор излагали, рассматривалось также и другими математиками, мы не можем обойти их заслуги молчанием. Относительно эквивалентности форм общее исследование произвел Л а г р а н ж, «*Nouv. Mém. de l'Ac. de Berlin*», 1773, p. 263; 1775, p. 323 и сл., где он, в частности, показал, что для каждого данного определителя имеется конечное число форм с тем свойством, что каждая форма с этим определителем эквивалентна одной из них и что тем самым все формы с данным определителем могут быть разбиты на классы. Позднее Л е ж а н д р открыл, в большинстве случаев индуктивным путем, многие изящные свойства этой классификации, которые мы ниже подкрепим доказательствами. Впрочем, до сих пор никто не входил в исследование собственной и несобственной эквивалентности, польза которого особенно обнаруживается в более тонких исследованиях.

Знаменитая проблема, изложенная в п. 216, была впервые решена Л а г р а н ж е м, «*Hist. de l'Ac. de Berlin*», 1767, p. 165; 1768, p. 181 и сл. Решение (менее совершенное) находится также в уже упоминавшихся ранее дополнениях к «*Алгебре*» Э й л е р а. Еще раньше на этот вопрос обратил внимание Э й л е р, «*Comm. Petr.*», T. VI, p. 175: «*Comm. Nov.*», T. IX, p. 3; там же, T. XVIII, p. 185 и сл.; однако он все время ограничивался в своем исследовании тем, что из одного решения, которое он предполагал уже известным, выводил другие, и, кроме того, его методы могли дать все решения только в немногих случаях (ср. L a g r a n g e, «*Hist. de l'Ac. de Berlin*», 1767, p. 237). Так как последнее из этих трех сочинений имеет дату более раннюю, чем сочинение Л а г р а н ж а, которое разбирает задачу во всей общности и не оставляет уже ничего желать в этом отношении, то Э й л е р в свое время (восьмидесятый том «*Комментариев*» относится к 1773 г. и опубликован в 1774 г.) еще не мог знать этого решения. Впрочем, наше решение (так же, как и все остальное, что мы до сих пор изложили в этом разделе) базируется на совершенно иных принципах.



То, что необходимо здесь сообщить о других — Д и о ф а н т е, Ф е р м а и т. д., — касается только частных случаев; так как то, что особенно достойно упоминания, мы уже указывали выше, мы не будем тратить силы на то, чтобы перечислять все подробности.

То, что мы до сих пор изложили о формах второй степени, следует рассматривать только как начало этой теории; при более усердном продолжении этого исследования нам открылось весьма широкое поле для изысканий, из которых то, что оказывается наиболее замечательным, мы изложим ниже. Действительно, этот предмет настолько плодотворен, что ради краткости мы должны обойти молчанием многое другое, что нами сейчас уже найдено; но намного больше остается еще, без сомнения, не открытым и ждет новых усилий. Кстати, мы хотим в начале этих исследований заметить, что формы с определителем 0 из рассмотрения исключаются, если только явно не оговорено противное.

## ДАЛЬНЕЙШИЕ ИССЛЕДОВАНИЯ О ФОРМАХ

### Разбиение форм с заданным определителем на классы

223

Выше (пп. 175, 195, 211) мы уже показали, что если задано какое-нибудь целое (положительное или отрицательное) число  $D$ , то можно указать конечное число форм  $F, F', F'', \dots$  с определителем  $D$ , обладающих тем свойством, что каждая форма с определителем  $D$  собственно эквивалентна одной и только одной из них. Тем самым все формы с определителем  $D$  (число которых бесконечно велико) могут быть разбиты на классы, именно, первый класс состоит из всех форм, которые собственно эквивалентны форме  $F$ , второй — из форм, которые собственно эквивалентны форме  $F'$  и т. д.

Из определенного класса форм с данным определителем может быть выбрана какая-нибудь форма, которая может рассматриваться как представитель всего класса. Вообще говоря, совершенно безразлично, какую форму выбирать из каждого класса, однако *предпо-*

чение всегда будет оказываться той форме, которая проще остальных. Простота какой-нибудь формы  $(a, b, c)$  выражается, очевидно, в величине чисел  $a, b, c$ , и форма  $(a', b', c')$  с полным правом может быть названа менее простой, чем  $(a, b, c)$ , если  $a' > a, b' > b, c' > c$ . Этим, однако, положение вещей еще не полностью определено, и, например, остается еще зависящим от нашего желания, какую из форм  $(17, 0 - 45), (5, 0, -153)$  считать более простой. По большей части, однако, бывает целесообразным соблюдать следующее правило.

I. Если определитель  $D$  отрицателен, то в качестве представителей нужно брать приведенные формы из каждого класса; если же в одном и том же классе находятся две приведенные формы (которые тогда противоположны, п. 172), то нужно брать ту из них, у которой средний член положителен.

II. Если определитель  $D$  есть положительное число, не являющееся квадратом, то нужно найти период какой-нибудь приведенной формы, содержащейся в заданном классе; в этом периоде будет или две двусторонние формы, или ни одной (п. 187).

1. В первом случае пусть  $(A, B, C), (A', B', C')$  двусторонние формы; далее, пусть наименьшие вычеты чисел  $B, B'$  по модулям  $A, A'$  соответственно равны  $M, M'$  (которые могут быть взяты положительными, если они не равны нулю), и, наконец,  $\frac{D - M^2}{A} = N, \frac{D - M'^2}{A'} = N'$ . Тогда в качестве представителя берется та из форм  $(A, M, -N), (A', M', -N')$ , которая проще. При этом предпочтение отдается той форме, у которой средний член равен нулю; если же средние члены или у обеих форм равны нулю, или ни у одной не равны нулю, то предпочитается та форма, которая имеет меньший первый член, а если первые члены по величине равны, но их знаки противоположны, то предпочтение отдается положительному знаку перед отрицательным.

2. Если же во всем периоде нет ни одной двусторонней формы, то среди всех форм периода выбирается та, которая имеет наименьший (не принимая во внимание знак) первый член, причем если в этом периоде имеется две формы, у которых один и тот же первый член, но у первой с положительным знаком, а у второй с отрицательным, то первой отдается предпочтение перед второй. Если эта форма есть

$(A, B, C)$  и из нее так же как и в предыдущем случае получена другая форма  $(A, M, -N)$  (именно, за  $M$  берется абсолютно наименьший вычет  $B$  по модулю  $A$ , и полагается  $N = \frac{D-M^2}{A}$ ), то эта последняя и берется в качестве представителя.

Если же случится, что один и тот же наименьший первый член встречается у нескольких форм периода, то все эти формы должны быть рассмотрены таким же образом, и из получающихся форм нужно взять в качестве представителя ту, у которой средний член наименьший.

Так, например, для  $D = 305$  среди других имеется следующий период:  $(17, 4, -17)$ ,  $(-17, 13, 8)$ ,  $(8, 11, -23)$ ,  $(-23, 12, 7)$ ,  $(7, 16, -7)$ ,  $(-7, 12, 23)$ ,  $(23, 11, -8)$ ,  $(-8, 13, 17)$ , из которого сначала выбирается форма  $(7, 16, -7)$ ; из нее выводится затем представитель  $(7, 2, -43)$ .

III. Если определитель является положительным квадратом и равен  $k^2$ , то отыскивается содержащаяся в заданном классе приведенная форма  $(A, k, 0)$ , и если  $A \leq k$ , то она и берется в качестве представителя; если же  $A > k$ , то вместо нее берется форма  $(A - 2k, k, 0)$ , первый член которой отрицателен, но меньше чем  $k$ .

Пример. Все формы с определителем  $-235$  распадаются на шестнадцать классов, представителями которых являются  $(1, 0, 235)$ ,  $(2, 1, 118)$ ,  $(4, 1, 59)$ ,  $(4, -1, 59)$ ,  $(5, 0, 47)$ ,  $(10, 5, 26)$ ,  $(13, 5, 20)$ ,  $(13, -5, 20)$ , и еще восемь других форм, которые отличаются от предыдущих только знаками крайних членов, именно,  $(-1, 0, -235)$ ,  $(-2, 1, -118)$ , ...

Все формы с определителем  $79$  распадаются на шесть классов, представителями которых являются формы  $(1, 0, -79)$ ,  $(3, 1, -26)$ ,  $(3, -1, -26)$ ,  $(-1, 0, 79)$ ,  $(-3, 1, 26)$ ,  $(-3, -1, 26)$ .

Таким образом, при этой классификации формы, которые собственно эквивалентны, полностью обособливаются от остальных. Две формы с одним и тем же определителем эквивалентны, если они принадлежат одному классу; каждое число, которое представляется одной из них, может быть представлено также и другой, и если какое-

нибудь число  $M$  может быть представлено первой формой так, что неизвестные имеют взаимно простые значения, то это число может быть представлено таким же образом и другой формой, причем так, что оба представления принадлежат одному и тому же значению выражения  $\sqrt{D} \pmod{M}$ . Если же две формы принадлежат к различным классам, то они не являются собственно эквивалентными; из представимости какого-нибудь заданного числа одной из форм нельзя заключить о представимости этого же числа и другой формой; наоборот, если число  $M$  может быть представлено одной из форм так, что значения неизвестных взаимно просты, то тотчас же ясно, что подобного представления этого числа другой формой, которое принадлежало бы тому же значению выражения  $\sqrt{D} \pmod{M}$ , быть не может (ср. пп. 167, 168).

Напротив, вполне возможно, что две формы  $F, F'$  из различных классов  $K, K'$  не собственно эквивалентны; в этом случае *каждая* форма из одного класса будет не собственно эквивалентна *каждой* форме из другого класса, каждая форма из  $K$  имеет противоположную себе форму в  $K'$ , и *классы  $K, K'$  сами будут называться противоположными*. Так, в первом примере предыдущего пункта третий класс форм с определителем — 235 противоположен четвертому, а седьмой — восьмому; во втором примере второй класс противоположен третьему, а пятый — шестому. Если поэтому даны какие-нибудь две формы из противоположных классов, то каждое число  $M$ , которое может быть представлено одной из них, будет представляться также и другой, причем если для первой формы представление достигается взаимно простыми значениями, то для второй возможно представление таким же образом, причем оба эти представления будут принадлежать противоположным значениям выражения  $\sqrt{D} \pmod{M}$ . Впрочем, указанные выше правила для выбора представителей таковы, что противоположные классы всегда имеют противоположных представителей.

Наконец, имеются также *классы, которые противоположны самим себе*. Именно, если какая-нибудь форма одновременно с противоположной ей формой содержится в одном и том же классе, то легко видеть, что все формы этого класса эквивалентны между собой как собственно, так и не собственно, и для каждой формы

встречается и ей противоположная. Таким будет каждый класс, в котором содержится двусторонняя форма, и наоборот, в каждом противоположном самому себе классе обязательно будет встречаться двусторонняя форма (пп. 163, 165), вследствие чего сам класс будет называться двусторонним. Так, среди классов форм с определителем —235 имеется восемь двусторонних, представителями которых являются  $(1, 0, 235)$ ,  $(2, 1, 118)$ ,  $(5, 0, 47)$ ,  $(10, 5, 26)$ ,  $(-1, 0, -235)$ ,  $(-2, 1, -118)$ ,  $(-5, 0, -47)$ ,  $(-10, 5, -26)$ ; среди классов форм с определителем 79 двусторонних два, представителями которых являются  $(1, 0, -79)$ ,  $(-1, 0, 79)$ . Впрочем, если представители определены по нашим правилам, то двусторонние классы могут быть найдены без труда. Именно, для положительного неквадратного определителя двусторонний класс будет, очевидно, иметь представителем двустороннюю форму (п. 194); для отрицательного определителя представители двусторонних классов будут или классами двусторонними, или такими, что их крайние члены равны (п. 172); наконец, для положительного квадратного определителя мы, согласно п. 210, легко убеждаемся, является ли представитель несобственно эквивалентным самому себе и потому является ли представляемый им класс двусторонним.

## 225

Выше (п. 175) мы уже показали, что у формы  $(a, b, c)$  с отрицательным определителем крайние члены имеют одинаковые знаки как между собой, так и со знаками крайних членов каждой эквивалентной ей формы. Если  $a, c$  положительны, то мы будем называть форму  $(a, b, c)$  положительной формой, и точно также будем называть весь класс, в котором содержится  $(a, b, c)$  и который состоит только из положительных форм, положительным классом. Наоборот,  $(a, b, c)$  будет отрицательной формой и будет содержаться в отрицательном классе, если  $a, c$  отрицательны. Положительной формой не могут представляться отрицательные числа, а отрицательной формой — положительные числа. Если  $(a, b, c)$  является представителем положительного класса, то форма  $(-a, b, -c)$

будет представителем отрицательного, откуда следует, что число положительных классов равно числу отрицательных и что если определены первые, то тем самым даны и вторые. Поэтому при исследовании форм с отрицательным определителем нужно, по большей части, рассматривать только положительные классы, так как их свойства легко переносятся на отрицательные классы.

Впрочем, такое различие характерно только для форм с отрицательным определителем; формами с положительным определителем могут представляться и положительные и отрицательные числа, и даже нередко в этом случае две формы вида  $(a, b, c)$ ,  $(-a, b, -c)$  принадлежат одному и тому же классу.

## Разбиение классов на порядки

226

Некоторую форму  $(a, b, c)$  мы будем называть **примитивной формой**, если числа  $a, b, c$  не имеют общих делителей; в противном случае она будет называться **произведенной формой**, причем если наибольший общий делитель чисел  $a, b, c$  равен  $m$ , то форма  $(a, b, c)$  произведена из примитивной формы  $(a/m, b/m, c/m)$ . Из этого определения тотчас же вытекает, что все формы, определители которых не делятся ни на какой квадрат, кроме 1, обязательно являются примитивными формами. Далее, из п. 161 следует, что если в какой-нибудь данный класс форм с определителем  $D$  входит примитивная форма, то все формы этого класса будут примитивными; в этом случае сам класс будет называться **примитивным**. Далее, ясно, что если какая-нибудь форма  $F$  с определителем  $D$  произведена из примитивной формы  $f$  с определителем  $D/m^2$ , и классы, в которых содержатся соответственно формы  $F, f$ , суть  $K, k$ , то все формы класса  $K$  могут быть произведены из примитивного класса  $k$ ; в этом случае мы будем называть поэтому сам класс  $K$  **произведенным из примитивного класса  $k$** .

Если форма  $(a, b, c)$  примитивная, но  $a, c$  не являются одновременно четными (т. е. если или они оба, или по крайней мере одно из них нечетно), то легко видеть, что не только  $a, b, c$ , но

и  $a$ ,  $2b$ ,  $c$  не могут иметь общих делителей, и в этом случае форма  $(a, b, c)$  будет называться **собственно примитивной** или *просто собственной формой*. Если же форма  $(a, b, c)$  примитивная и числа  $a$ ,  $c$  оба четные, то очевидно, что числа  $a$ ,  $2b$ ,  $c$  будут иметь общий делитель 2 (который одновременно будет наибольшим), и тогда  $(a, b, c)$  будет называться **несобственно примитивной**, или *просто несобственной формой* \*. В этом случае  $b$  обязательно нечетно (так как иначе форма  $(a, b, c)$  не была бы примитивной формой); поэтому  $b^2 \equiv 1 \pmod{4}$  и тем самым, так как  $ac$  делится на 4, определитель  $b^2 - ac \equiv 1 \pmod{4}$ . Несобственные формы имеются поэтому только для определителя вида  $4n + 1$ , если он положителен, или вида  $-(4n + 3)$ , если он отрицателен. Из п. 161, однако, очевидно, что если в каком-нибудь данном классе находится собственно примитивная форма, то все формы этого класса собственно примитивны, и, наоборот, что класс, который содержит одну несобственно примитивную форму, сплошь состоит из несобственно примитивных форм. Поэтому *сам класс в первом случае будет называться собственно примитивным классом или просто собственным классом, а во втором случае несобственно примитивным или просто несобственным классом*. Так, например, среди положительных классов форм с определителем  $-235$  имеется шесть собственных классов, именно, тех, представителями которых являются  $(1, 0, 235)$ ,  $(4, 1, 59)$ ,  $(4, -1, 59)$ ,  $(5, 0, 47)$ ,  $(13, 5, 20)$ ,  $(13, -5, 20)$  и столько же имеется их среди отрицательных классов. Несобственных же классов будет и тут и там по два. Классы форм с определителем 79 (это число имеет вид  $4n + 3$ ) все являются собственными.

Если форма  $(a, b, c)$  является произведенной, причем из примитивной формы  $(a/t, b/t, c/t)$ , то последняя может быть или собственно, или несобственно примитивной. В первом случае  $t$

---

\* Мы остановились на выражениях «собственная» и «несобственная», потому что не нашли ничего более удобного; мы указываем на это для того, чтобы кто-либо не стал искать связи между этим обозначением и тем, которое употребляется начиная с. п. 157, ибо такой связи нет. Впрочем, на каких недоразумений на этой почве возникнуть, разумеется, не может.



является также наибольшим общим делителем чисел  $a$ ,  $2b$ ,  $c$ ; во втором случае наибольший общий делитель этих чисел будет равен  $2m$ . Этим самым делается понятным различие между *формой, произведенной из собственно примитивной формы*, и *формой, произведенной из несобственно примитивной формы*, и точно так же (ибо, согласно п. 161, все формы одного и того же класса тоже находятся в этой связи) между *классом, произведенным из собственно примитивного класса*, и *классом, произведенным из несобственно примитивного класса*.

Посредством этого различия мы получили первую основу, на которой может быть построено *разбиение всех классов форм с заданным определителем на различные порядки*. Два класса, представителями которых являются формы  $(a, b, c)$ ,  $(a', b', c')$ , мы будем причислять к *одному и тому же порядку*, если как числа  $a, b, c$  имеют тот же самый наибольший общий делитель, что  $a', b', c'$ , так и числа  $a, 2b, c$  имеют тот же наибольший общий делитель, что  $a', 2b', c'$ . Если же одно или другое, или оба эти условия не имеют места, то мы будем причислять классы к *различным порядкам*. Отсюда тотчас же вытекает, что все собственно примитивные формы образуют один порядок, а все несобственно примитивные формы — другой порядок. Если  $m^2$  является квадратом, входящим в определитель  $D$ , то классы, произведенные из собственно примитивных классов с определителем  $D/m^2$ , будут образовывать отдельный порядок, произведенные из несобственно примитивных классов с определителем  $D/m^2$  — другой порядок и т. д. Если случайно  $D$  не делится ни на какой квадрат (кроме 1), то порядков из произведенных классов не будет, и потому будет или один порядок (если  $D \equiv 2$  или  $3$  по модулю 4), именно, порядок собственно примитивных классов, или два порядка (если  $D \equiv 1 \pmod{4}$ ), именно, порядок собственно примитивных и порядок несобственно примитивных классов. При помощи комбинаторных соображений без труда обосновывается следующее **общее правило**. Если  $D = D' 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \dots$ , где  $D'$  не содержит квадратных сомножителей, и  $a, b, c, \dots$  — различные нечетные простые числа (в таком виде может быть представлено каждое число, если положить  $\mu = 0$ , когда  $D$  не делится на 4, и положить равными 0 все  $\alpha, \beta, \gamma, \dots$



или, что то же самое, отбросить сомножители  $a^{2\alpha}$ ,  $b^{2\beta}$ ,  $c^{2\gamma}$ , ..., когда  $D$  не делится ни на какой нечетный квадрат), то имеется или  $(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$  порядков, именно, когда  $D' \equiv 2$  или  $3 \pmod{4}$ , или  $(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$  порядков, именно, когда  $D' \equiv 1 \pmod{4}$ .

Доказательство этого правила, мы, однако, опустим, так как оно не является ни трудным, ни очень уж здесь необходимым.

**Пример 1.** Для  $D = 45 = 5 \cdot 3^2$  имеется шесть классов, представителями которых являются формы  $(1, 0, -45)$ ,  $(-1, 0, 45)$ ,  $(2, 1, -22)$ ,  $(-2, 1, 22)$ ,  $(3, 0, -15)$ ,  $(6, 3, -6)$ . Они распадаются на четыре порядка: именно, первый порядок охватывает оба собственных класса, представители которых суть  $(1, 0, -45)$  и  $(-1, 0, 45)$ ; второй порядок будет содержать оба несобственных класса с представителями  $(2, 1, -22)$  и  $(-2, 1, 22)$ ; третий порядок содержит только один класс, произведенный из собственного класса с определителем 5, именно, тот, представителем которого является  $(3, 0, -15)$ , и, наконец, четвертый порядок состоит из одного произведенного из несобственного класса с определителем 5 класса, представитель которого есть  $(6, 3, -6)$ .

**Пример 2.** Положительные классы с определителем  $-99 = -11 \cdot 3^2$  распадаются на четыре порядка. Первый порядок охватывает следующие собственно примитивные классы \*:  $(1, 0, 99)$ ,  $(4, 1, 25)$ ,  $(4, -1, 25)$ ,  $(5, 1, 20)$ ,  $(5, -1, 20)$ ,  $(9, 0, 11)$ ; второй порядок содержит несобственные классы  $(2, 1, 50)$ ,  $(10, 1, 10)$ ; третий порядок содержит классы  $(3, 0, 33)$ ,  $(9, 3, 12)$ ,  $(9, -3, 12)$ , произведенные из собственных классов с определителем  $-11$ ; четвертый — один единственный класс  $(6, 3, 18)$ , произведенный из несобственного класса с определителем  $-11$ . Отрицательные классы этого определителя могут быть разбиты на порядки точно таким же образом.

Заметим, что *противоположные классы всегда принадлежат одному и тому же порядку*, факт, причина которого видна без труда.

---

\* Ради краткости мы вместо самих классов указываем их представителей.

Из этих различных порядков *наибольшего внимания заслуживает порядок собственно примитивных классов*. Действительно, отдельные произведенные классы получаются из некоторых примитивных классов (с меньшим определителем), из рассмотрения которых часто сами собой получаются факты, касающиеся первых. Но ниже мы покажем, что каждый несобственно примитивный класс может быть в некотором смысле ассоциирован или с одним собственно примитивным классом (с тем же определителем), или с тремя. Далее, при отрицательном определителе отрицательные классы могут быть оставлены в стороне, так как каждому из них всегда соответствует некоторый положительный класс. Чтобы теперь глубже проникнуть в природу собственно примитивных классов, мы прежде всего введем между ними одно существенное различие, по которому весь порядок собственных классов может быть разделен на несколько родов. Так как до сих пор мы еще не касались этого очень важного предмета, мы должны изложить все с самого начала

## Деление порядков на роды

**Теорема.** *Посредством любой собственно примитивной формы  $F$  может быть представлено бесконечно много чисел, которые не делятся на заданное простое число  $p$ .*

**Доказательство.** Если форма есть  $F = ax^2 + 2bxy + cy^2$ , то  $p$ , очевидно, не может одновременно входить во все три числа  $a$ ,  $2b$ ,  $c$ . Если теперь  $a$  не делится на  $p$ , то ясно, что если для  $x$  взять какое-нибудь число, не делящееся на  $p$ , а для  $y$  — делящееся на  $p$ , то значение формы  $F$  на  $p$  не делится; если же  $c$  не делится на  $p$ , то мы добьемся того же, если придадим  $x$  значение, делящееся на  $p$ , а  $y$  — не делящееся на  $p$ ; если, наконец,  $a$  и  $c$  делятся на  $p$ , и потому  $2b$  не делится на  $p$ , то форма  $F$  будет принимать не делящиеся на  $p$  значения, если и  $x$  и  $y$  придавать значения, не делящиеся на  $p$ .

Очевидно, теорема будет сохранять силу и для несобственно примитивных форм, если только  $p$  не равно 2.

Так как одновременно могут выполняться многие такие условия, именно, что одно и то же число должно делиться на некоторые заданные простые числа и не делиться на другие (ср. п. 32), то легко видеть, что числа  $x, y$  могут быть бесконечным числом способов определены так, что примитивная форма  $ax^2 + 2bxy + cy^2$  принимает значение, которое не делится на любое количество заданных простых чисел, из которых исключается одно единственное число 2, если форма несобственно примитивна. Отсюда вытекает, что в более общем виде теорема может быть высказана следующим образом.

Посредством любой примитивной формы может быть представлено бесконечно много чисел, которые взаимно просты с заданным (нечетным, если форма несобственно примитивна) числом.

## 229

**Теорема.** Если  $F$  — примитивная форма с определителем  $D$ , и  $p$  — входящее в  $D$  простое число, то не делящиеся на  $p$  числа, которые могут быть представлены формой  $F$ , обладают тем общим свойством, что либо все они являются квадратичными вычетами, либо все квадратичными невычетами по модулю  $p$ .

**Доказательство.** Если  $F = (a, b, c)$  и, далее,  $m, m'$  — какие-нибудь два числа, не делящиеся на  $p$ , которые могут быть представлены формой  $F$ , именно,

$$m = ag^2 + 2bgh + ch^2, \quad m' = ag'^2 + 2bg'h' + ch'^2,$$

то

$$mm' = [agg' + b(gh' + hg') + chh']^2 - D(gh' - hg')^2;$$

тем самым произведение  $mm'$  сравнимо с квадратом по модулю  $D$ , а потому также и по модулю  $p$ , т. е.  $mm'$  есть квадратичный вычет по модулю  $p$ . Отсюда следует, что или каждое из чисел  $m, m'$  является квадратичным вычетом, или каждое является квадратичным невычетом по модулю  $p$ .

Подобным же образом доказывается, что если определитель  $D$  делится на 4, то представляющиеся формой  $F$  нечетные числа или все  $\equiv 1$ , или все  $\equiv 3 \pmod{4}$ . Действительно, в этом случае произведение двух таких чисел всегда будет квадратичным вычетом по модулю 4, и потому  $\equiv 1 \pmod{4}$ ; поэтому либо каждое из них  $\equiv 1$ , либо оба  $\equiv 3$ .

Если, наконец,  $D$  делится на 8, то произведение двух любых нечетных чисел, которые могут быть представлены формой  $F$ , является квадратичным вычетом по модулю 8 и потому оно  $\equiv 1 \pmod{8}$ . Поэтому в этом случае представляющиеся формой  $F$  нечетные числа или все  $\equiv 1$ , или все  $\equiv 3$ , или все  $\equiv 5$ , или все  $\equiv 7 \pmod{8}$ .

Так, например, так как число 10, которое является невычетом по модулю 7, может быть представлено формой  $(10, 3, 17)$ , то все не делящиеся на 7 числа, которые могут быть представлены этой формой, являются невычетами по модулю 7. Так как  $-3$  представляется формой  $(-3, 1, 49)$  и  $\equiv 1 \pmod{4}$ , то все представляющиеся этой формой нечетные числа будут обладать тем же свойством.

Впрочем, мы могли бы, если бы это было необходимо для наших целей, легко доказать, что представляемые формой  $F$  числа не находятся в постоянном отношении такого рода ни с одним простым числом, не входящим в  $D$ , т. е. что как вычеты, так и невычеты каждого не входящего в  $D$  простого числа могут быть представлены формой  $F$ . Наоборот, в отношении чисел 4 и 8 нечто аналогичное имеет место и в других случаях, и мимо этого мы пройти не можем.

1. Если определитель  $D$  примитивной формы  $F$  сравним с 3  $\pmod{4}$ , то нечетные числа, представляющиеся формой  $F$ , будут или все  $\equiv 1$ , или все  $\equiv 3 \pmod{4}$ . Именно, если  $m, m'$  — два представляемых формой  $F$  числа, то произведение  $mm'$  может быть тем же способом, как выше, представлено в виде  $p^2 - Dq^2$ . Если поэтому каждое из чисел  $m, m'$  нечетно, то обязательно одно из чисел  $p, q$  должно быть четным, а другое нечетным, а потому из двух квадратов  $p^2, q^2$  один  $\equiv 0$ , а другой  $\equiv 1 \pmod{4}$ . Отсюда легко следует, что  $p^2 - Dq^2 \equiv 1 \pmod{4}$ , и потому числа  $m, m'$  или

оба  $\equiv 1$ , или оба  $\equiv 3 \pmod{4}$ . Так, например, формой  $(10, 3, 17)$  не могут быть представлены никакие нечетные числа, кроме имеющих вид  $4n + 1$ .

II. Если определитель  $D$  примитивной формы  $F$  сравним с  $2 \pmod{8}$ , то нечетные числа, представляющиеся формой  $F$ , будут или все либо  $\equiv 1$ , либо  $\equiv 7$ , или все либо  $\equiv 3$ , либо  $\equiv 5 \pmod{8}$ . Действительно, пусть  $m, m'$  — два представляющихся формой  $F$  нечетных числа, произведение которых тем самым может быть представлено в виде  $p^2 - Dq^2$ . Тогда, так как оба числа  $m, m'$  нечетны, то  $p$  обязательно должно быть нечетно (так как  $D$  четно), и потому  $p^2 \equiv 1 \pmod{8}$ ; а  $q^2$  или  $\equiv 0$ , или  $\equiv 1$ , или  $\equiv 4$ , и потому  $Dq^2$  или  $\equiv 0$ , или  $\equiv 2$ . Поэтому  $mm' = p^2 - Dq^2$  будет или  $\equiv 1$ , или  $\equiv 7 \pmod{8}$ . Таким образом, если  $m$  или  $\equiv 1$ , или  $\equiv 7$ , то и  $m'$  будет или  $\equiv 1$ , или  $\equiv 7$ , а если  $m$  или  $\equiv 3$ , или  $\equiv 5$ , то и  $m'$  будет или  $\equiv 3$ , или  $\equiv 5$ . Так, например, все нечетные числа, представляющиеся формой  $(3, 1, 5)$ , или  $\equiv 3$ , или  $\equiv 5 \pmod{8}$ , а ни одно число вида  $8n + 1$  или  $8n + 7$  этой формой представлено быть не может.

III. Если определитель  $D$  примитивной формы  $F$  сравним с  $6 \pmod{8}$ , то этой формой могут быть представлены нечетные числа или только такого рода, которые  $\equiv 1$  и  $\equiv 3 \pmod{8}$ , или только такого рода, которые  $\equiv 5$  и  $\equiv 7 \pmod{8}$ . Доказательство, которое совершенно аналогично предыдущему (в II), каждый может провести без труда. Так, например, формой  $(5, 1, 7)$  могут быть представлены только такие нечетные числа, которые или  $\equiv 5$ , или  $\equiv 7 \pmod{8}$ .

### 230

Поэтому все числа, которые могут быть представлены заданной примитивной формой  $F$ , с определителем  $D$ , будут находиться во вполне определенной связи с отдельными простыми делителями  $D$  (на которые сами они делиться не могут); нечетные же числа, которые могут быть представлены формой  $F$ , в некоторых случаях будут иметь определенное отношение также и к числам 4 и 8, именно, к числу 4, если  $D$  или  $\equiv 0$ , или  $\equiv 3 \pmod{4}$ , и к числу 8,

если  $D$  или  $\equiv 0$ , или  $\equiv 2$ , или  $\equiv 6 \pmod{8}$  \*. *Отношение такого рода к этим отдельным числам мы будем называть характером или специальным характером формы  $F$  и выражать его следующим образом: если формой  $F$  могут быть представлены только квадратичные вычеты простого числа  $p$ , то мы будем придавать ей характер  $Rp$ , в противном случае — характер  $Np$ ; аналогично мы будем писать 1, 4, если формой  $F$  не могут быть представлены другие нечетные числа, кроме тех, которые  $\equiv 1 \pmod{4}$ , из чего тотчас же вытекает, какие характеры будут выражаться обозначениями 3, 4; 1, 8; 3, 8; 5, 8; 7, 8. Наконец, формам, которыми могут представляться только такие нечетные числа, которые по модулю 8 или  $\equiv 1$ , или  $\equiv 7$ , мы будем придавать характер 1 и 7, 8, из чего само собой получается значение характеров 3 и 5, 8; 1 и 3, 8; 5 и 7, 8.*

*Отдельные характеры заданной примитивной формы  $(a, b, c)$  с определителем  $D$  всегда могут быть определены по крайней мере по одному из чисел  $a, c$  (которые оба, очевидно, представляются этой формой). Действительно, если  $p$  — простой делитель  $D$ , то одно из чисел  $a, c$ , очевидно, не будет делиться на  $p$ ; в самом деле, если бы оба они делились на  $p$ , то  $p$  входило бы также и в  $b^2 (= D + ac)$ , а значит и в  $b$ , т. е. форма  $(a, b, c)$  не была бы примитивной. Аналогичным образом, в тех случаях, когда форма  $(a, b, c)$  имеет определенное отношение к числу 4 или 8, то по крайней мере одно из чисел  $a, c$ , очевидно, будет нечетным, а по нему и можно будет узнать это отношение. Так, например, для формы  $(7, 0, 23)$  по отношению к числу 23 из числа 7 получается характер  $N23$ ; по отношению к числу 7 из числа 23 для этой же формы получается характер  $R7$ ; наконец, характер этой формы по отношению к числу 4, именно, 3, 4, может быть получен как из числа 7, так и из числа 23.*

Все числа, которые могут быть представлены какой-нибудь формой  $F$ , содержащейся в классе  $K$ , представимы также и всякой другой формой этого класса, и потому, очевидно, отдельные характеры формы  $F$  будут принадлежать и всем остальным формам этого класса, вследствие чего их можно рассматривать как характеры

---

\* Для определителей, делящихся на 8, отношение их к числу 4 можно не рассматривать, так как оно уже определяется отношением к числу 8.

всего класса. Поэтому отдельные характеры любого заданного примитивного класса можно узнать по его представителю. Противоположные классы всегда будут иметь все характеры одинаковые.

## 231

Совокупность всех специальных характеров заданной формы или класса образует **полный характер** этой формы или класса. Так, например, полный характер формы  $(10, 3, 17)$  или всего представляемого ею класса есть  $1, 4; N7; N23$ . Подобным же образом полный характер формы  $(7, -1, 17)$  есть  $7, 8; R3; N5$ ; действительно, специальный характер  $3, 4$  в этом случае отбрасывается, так как уже содержится в характере  $7, 8$ . На этом мы основываем деление всего порядка собственно примитивных (если определитель отрицателен, то положительных) классов с данным определителем на несколько различных родов, именно, все классы, которые имеют один и тот же полный характер, мы причисляем к одному роду, а классы, полные характеры которых различны, — к различным родам. Отдельным же классам мы придаем тот полный характер, который имеют содержащиеся в них отдельные формы. Так, например, для определителя  $-161$  получается шестнадцать собственно примитивных положительных классов, которые следующим образом разбиваются на четыре рода:

| характер        | формы, представляющие классы                         |
|-----------------|------------------------------------------------------|
| $1, 4; R7; R23$ | $(1, 0, 161), (2, 1, 81), (9, 1, 18), (9, -1, 18)$   |
| $1, 4; N7; N23$ | $(5, 2, 33), (5, -2, 33), (10, 3, 17), (10, -3, 17)$ |
| $3, 4; R7; N23$ | $(7, 0, 23), (11, 2, 15), (11, -2, 15), (14, 7, 15)$ |
| $3, 4; N7; R23$ | $(3, 1, 54), (3, -1, 54), (6, 1, 27), (6, -1, 27).$  |

Относительно числа различных полных характеров, которые возможны а priori, можно заметить следующее.

I. Если определитель делится на 8, то по отношению к числу 8 возможны четыре различных специальных характера; число 4

не дает никаких специальных характеров (замечание к предыдущему пункту). Кроме того, по отношению к каждому из отдельных нечетных простых делителей числа  $D$  имеется по два характера. Если поэтому число таких делителей равно  $m$ , то всего будет  $2^{m+2}$  различных полных характеров (где нужно положить  $m = 0$ , если  $D$  есть степень числа 2).

II. Если определитель  $D$  не делится на 8, но делится на 4, и, кроме того, на  $m$  нечетных простых чисел, то всего имеется  $2^{m+1}$  различных полных характеров.

III. Если определитель  $D$  четен, но не делится на 4, то он или  $\equiv 2$ , или  $\equiv 6 \pmod{8}$ . В первом случае имеется два специальных характера по отношению к числу 8, именно, 1 и 7, 8; 3 и 5, 8; во втором случае — столько же. Если поэтому положить количество нечетных простых делителей числа  $D$  равным  $m$ , то всего будет  $2^{m+1}$  различных полных характеров.

IV. Если  $D$  нечетно, то оно или  $\equiv 1$ , или  $\equiv 3 \pmod{4}$ . Во втором случае по отношению к числу 4 имеется два различных характера, в то время как в первом случае подобное соотношение в полный характер не входит. Если поэтому  $m$  обозначает то же, что и раньше, то в первом случае имеется  $2^m$ , а во втором —  $2^{m+1}$  различных полных характеров.

Впрочем, нужно заметить, что отсюда никак не следует, что в действительности имеется столько же родов, сколько возможно различных характеров. В нашем примере только половине из них действительно соответствуют классы или роды, в то время как не существует положительных классов, имеющих характеры 1, 4;  $R7$ ;  $N23$  или 1, 4;  $N7$ ;  $R23$  или 3, 4;  $R7$ ;  $R23$  или 3, 4;  $N7$ ;  $N23$ . Об этом очень важном вопросе ниже будет сказано подробнее.

Форму  $(1, 0, -D)$ , которая, без сомнения, является простейшей среди всех форм с определителем  $D$ , мы будем отныне называть главной формой, весь класс, в который входит эта форма, — главным классом, и, наконец, весь род, в котором содержится главный класс, — главным родом. Поэтому нужно делать различие между главной формой, формой из главного класса и формой из главного рода; точно так же — между главным классом и классом из главного рода. Мы будем придерживаться этих наименований



всегда, даже и тогда, когда для какого-нибудь определителя случайно не будет других классов, кроме главного класса или других родов, кроме главного рода, как это, например, по большей части бывает, если  $D$  есть положительное простое число вида  $4n + 1$ .

## 232

Хотя то, что было изложено о характерах форм, первоначально служило только той цели, чтобы обосновать на этом подразделение *положительного собственно примитивного* порядка, ничто не мешает нам распространить это также и на отрицательные или несобственно примитивные формы и классы, и подразделить по такому же принципу на роды как положительный несобственно примитивный порядок, так и отрицательный собственно примитивный порядок и отрицательный несобственно примитивный порядок. Так, например, после того как собственно примитивный порядок форм с определителем 145 разложен на следующие два рода:

|           |                              |
|-----------|------------------------------|
| $R5; R29$ | $(1, 0, -145), (5, 0, -29)$  |
| $N5; N29$ | $(3, 1, -48), (3, -1, -48),$ |

то и несобственно примитивный порядок подобным же образом разбивается на два рода:

|           |                              |
|-----------|------------------------------|
| $R5; R29$ | $(4, 1, -36), (4, -1, -36)$  |
| $N5; N29$ | $(2, 1, -72), (10, 5, -12),$ |

или, подобно тому как положительные классы форм с определителем  $-129$  распадаются на четыре рода:

|                 |                                          |
|-----------------|------------------------------------------|
| $1, 4, R3; R43$ | $(1, 0, 129), (10, 1, 13), (10, -1, 13)$ |
| $1, 4; N3; N43$ | $(2, 1, 65), (5, 1, 26), (5, -1, 26)$    |
| $3, 4; R3; N43$ | $(3, 0, 43), (7, 2, 19), (7, -2, 19)$    |
| $3, 4; N3; R43$ | $(6, 3, 23), (11, 5, 14), (11, -5, 14),$ |

так и отрицательные классы делятся на четыре рода:

|               |                                              |
|---------------|----------------------------------------------|
| 3, 4; N3; N43 | (—1, 0, —129), (—10, 1, —13), (—10, —1, —13) |
| 3, 4; R3; R43 | (—2, 1, —65), (—5, 1, —26), (—5, —1, —26)    |
| 1, 4; N3; R43 | (—3, 0, —43), (—7, 2, —19), (—7, —2, —19)    |
| 1, 4; R3; N43 | (—6, 3, —23), (—11, 5, —14), (—11, —5, —14). |

Так как, однако, система отрицательных классов всегда подобна системе положительных классов, то в большинстве случаев было бы излишне рассматривать первую отдельно. А то, как несобственно примитивный порядок может быть сведен к собственно примитивному, мы покажем позднее.

Наконец, что касается произведенных порядков, то для их подразделения новых правил не требуется. Действительно, так как каждый произведенный порядок получается из некоторого примитивного порядка (меньшего определителя) и отдельные классы первого возникают из отдельных классов второго, то очевидно, что подразделение произведенного порядка может быть выведено из подразделения примитивного порядка.

### 233

Если (примитивная) форма  $F = (a, b, c)$  обладает тем свойством, что могут быть найдены два числа  $g, h$ , для которых  $g^2 \equiv a$ ,  $gh \equiv b$ ,  $h^2 \equiv c$  по некоторому заданному модулю  $m$ , то мы будем называть эту форму *квадратичным вычетом числа  $m$* , а  $gx + hy$  — значение выражения  $\sqrt{ax^2 + 2bxy + cy^2} \pmod{m}$  или, короче,  $(g, h)$  — значение выражения  $\sqrt{(a, b, c)}$ , или  $\sqrt{F} \pmod{m}$ . Более общо, если имеется взаимно простой с модулем  $m$  множитель  $M$  с тем свойством, что

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m},$$

то мы будем говорить, что  $M(a, b, c)$  или  $MF$  есть квадратичный вычет числа  $m$ , и  $(g, h)$  — значение выражения  $\sqrt{M(a, b, c)}$ , или  $\sqrt{MF} \pmod{m}$ . Так, например, форма  $(3, 1, 54)$  является квадратичным вычетом числа 23, и  $(7, 10)$  есть значение выражения

$\sqrt{(3, 1, 54)} \pmod{23}$ : аналогично,  $(2, -4)$  есть значение выражения  $\sqrt{5(10, 3, 17)} \pmod{23}$ . Польза этих определений будет показана позднее; здесь мы хотим только вывести следующие теоремы.

I. Если  $M(a, b, c)$  — квадратичный вычет числа  $m$ , то он будет входить в определитель формы  $(a, b, c)$ . Действительно, если  $(g, h)$  есть значение выражения  $\sqrt{M(a, b, c)} \pmod{m}$  или

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m},$$

то  $b^2M^2 - acM^2 \equiv 0$ , т. е.  $(b^2 - ac)M^2$  делится на  $m$ . Так как, однако,  $M$  предполагается взаимно простым с  $m$ , то и  $b^2 - ac$  будет делиться на  $m$ .

II. Если  $M(a, b, c)$  — квадратичный вычет числа  $m$ , и  $m$  или простое число, или степень простого числа, скажем, равно  $p^\mu$ , то специальный характер формы  $(a, b, c)$  по отношению к числу  $p$  будет  $Rp$  или  $Np$ , в зависимости от того, является ли  $M$  вычетом или невычетом по модулю  $p$ . Это сразу следует из того, что как  $aM$ , так и  $cM$  есть квадратичный вычет по модулю  $m$  или  $p$ , и по меньшей мере одно из чисел  $a, c$  не делится на  $p$  (п. 230).

Аналогичным образом, если  $m = 4$  (в то время как все остальное остается без изменений), то специальным характером формы  $(a, b, c)$  будет 1, 4 или 3, 4, в зависимости от того,  $M \equiv 1$  или  $\equiv 3$ ; далее, если  $m = 8$  или более высокой степени числа 2, то специальным характером формы  $(a, b, c)$  будет 1, 8; 3, 8; 5, 8; 7, 8, если соответственно  $M \equiv 1; 3; 5; 7 \pmod{8}$ .

III. Обратно, если  $m$  — простое число или степень простого числа, скажем,  $p^\mu$ , причем  $p$  входит в определитель  $b^2 - ac$  и, далее,  $M$  является вычетом или невычетом по модулю  $p$  в зависимости от того, каков характер формы  $(a, b, c)$  по отношению к  $p$ ,  $Rp$  или  $Np$ , то  $M(a, b, c)$  будет квадратичным вычетом числа  $m$ . Действительно, если  $a$  не делится на  $p$ , то  $aM$  будет вычетом по модулю  $p$ , а потому и по модулю  $m$ ; если  $g$  — значение выражения  $\sqrt{aM} \pmod{m}$ ,  $h$  — значение выражения  $bg/a \pmod{m}$ , то будет  $g^2 \equiv aM$ ,  $ah \equiv bg$ , и потому

$$agh \equiv bg^2 \equiv abM \quad \text{и} \quad gh \equiv bM;$$

наконец,

$$ah^2 \equiv bgh \equiv b^2M \equiv b^2M - (b^2 - ac)M \equiv acM,$$

и тем самым  $h^2 \equiv cM$ , т. е.  $(g, h)$  есть значение выражения  $\sqrt{M(a, b, c)}$ . Если же  $a$  делится на  $m$ , то  $c$ , очевидно, не делится; отсюда легко видно, что мы придем к тому же результату, если возьмем для  $h$  значение выражения  $\sqrt{cM} \pmod{m}$ , а для  $g$  — значение выражения  $bh/c \pmod{m}$ .

Аналогичным образом доказывается, что если  $m = 4$  и входит в  $b^2 - ac$ , и если, далее,  $M \equiv 1$  или  $\equiv 3$ , в зависимости от того, является ли специальным характером формы  $(a, b, c)$  1, 4 или 3, 4, то  $M(a, b, c)$  будет квадратичным вычетом числа  $m$ . Точно так же, если  $m = 8$  или является более высокой степенью числа 2, на которую делится  $b^2 - ac$ , и если, далее, предполагается  $M \equiv 1; 3; 5; 7 \pmod{8}$  в зависимости от того, чего требует специальный характер формы  $(a, b, c)$  по отношению к числу 8, то  $M(a, b, c)$  есть квадратичный вычет числа  $m$ .

IV. Если определитель формы  $(a, b, c)$  равен  $D$  и  $M(a, b, c)$  есть квадратичный вычет числа  $D$ , то по числу  $M$  могут быть сразу определены все специальные характеры формы  $(a, b, c)$  как по отношению к отдельным нечетным простым делителям  $D$ , так и по отношению к числу 4 или числу 8 (если они входят в  $D$ ). Так, например, так как 3 (20, 10, 27) есть квадратичный вычет числа 440, именно, значением  $\sqrt{3(20, 10, 27)} \pmod{440}$  является (150, 9), и 3N5, 3R11, то характеры формы (20, 10, 27) следующие: 3, 8; N5; R11. Только специальные характеры по отношению к числам 4 и 8, если последние не входят в определитель, не находятся ни в какой обязательной связи с числом  $M$ .

V. Обратно, если взаимно простое с  $D$  число  $M$  содержит в себе все специальные характеры формы  $(a, b, c)$  (за исключением характеров по отношению к числам 4 и 8, если они не входят в  $D$ ), то  $M(a, b, c)$  будет квадратичным вычетом числа  $D$ . Действительно, из III получается, что если число  $D$  представлено в виде  $\pm A^\alpha B^\beta C^\gamma \dots$ , где  $A, B, C, \dots$  — различные простые числа, то  $M(a, b, c)$  является квадратичным вычетом отдельных чисел  $A^\alpha, B^\beta, C^\gamma, \dots$ . Если поэтому  $(\mathfrak{A}, \mathfrak{A}')$  — значение выражения  $\sqrt{M(a, b, c)}$

по модулю  $A^\alpha$ ,  $(\mathfrak{B}, \mathfrak{B}')$  — значение этого же выражения по модулю  $B^\beta$ ,  $(\mathfrak{C}, \mathfrak{C}')$  — по модулю  $C^\gamma$  и т. д., и числа  $g, h$  определены так, что  $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots, h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \dots$  соответственно по модулям  $A^\alpha, B^\beta, C^\gamma, \dots$  (п. 32), то легко видеть, что  $g^2 \equiv aM, gh \equiv bM, h^2 \equiv cM$  по всем модулям  $A^\alpha, B^\beta, C^\gamma, \dots$ , а потому и по модулю  $D$ , который является их произведением.

VI. На основании этого числа, подобные  $M$ , называются характеристическими числами формы  $(a, b, c)$ , и, согласно V, несколько таких чисел может быть найдено без труда, если известны все специальные характеры этой формы; простейшие из них в большинстве случаев легче всего находить посредством проб. Очевидно, что если  $M$  — характеристическое число заданной примитивной формы с определителем  $D$ , то все числа, которые сравнимы с  $M$  по модулю  $D$ , также будут характеристическими числами этой же формы; далее, формы, содержащиеся в одном и том же классе, а также в различных классах одного и того же рода, имеют одни и те же характеристические числа, откуда следует, что каждое характеристическое число заданной формы может быть придано также целому классу или целому роду; наконец, 1 всегда есть характеристическое число главной формы, главного класса и главного рода, т. е. каждая форма из главного рода является квадратичным вычетом своего определителя.

VII. Если  $(g, h)$  есть значение выражения  $\sqrt{M(a, b, c)} \pmod{m}$ , и  $g' \equiv g, h' \equiv h \pmod{m}$ , то и  $(g', h')$  будет значением этого же выражения. Подобные значения могут рассматриваться как эквивалентные; если же  $(g, h), (g', h')$  — такие значения выражения  $\sqrt{M(a, b, c)} \pmod{m}$ , что не имеет места одновременно  $g' \equiv g, h' \equiv h \pmod{m}$ , то эти значения нужно считать различными. Очевидно, что если  $(g, h)$  — значение такого выражения, то таковым будет и  $(-g, -h)$ , и легко показать, что эти значения всегда различны, кроме случая  $m = 2$ . Точно так же легко показать, что выражение  $\sqrt{M(a, b, c)} \pmod{m}$  не может иметь больше различных значений, чем два (противоположных), если  $m$  равно или нечетному простому числу, или степени нечетного простого числа, или числу 4; если же  $m = 8$  или является более высокой степенью числа 2, то всего значений будет четыре. Отсюда при помощи VI

легко получается, что если определитель  $D$  формы  $(a, b, c)$  равен  $\pm 2^\mu A^\alpha B^\beta \dots$ , где  $A, B, \dots$  обозначают различные нечетные простые числа, количество которых пусть равно  $n$ , и если  $M$  — характеристическое число этой формы, то всего имеется или  $2^n$ , или  $2^{n+1}$ , или  $2^{n+2}$  различных значений выражения  $\sqrt{M(a, b, c)} \pmod{D}$ , в зависимости от того,  $\mu < 2$  или  $= 2$ , или  $> 2$ . Так, например, получается шестнадцать значений выражения  $\sqrt{7(12, 6, -17)} \pmod{240}$ , именно,  $(\pm 18, \mp 11)$ ,  $(\pm 18, \pm 29)$ ,  $(\pm 18, \mp 91)$ ,  $(\pm 18, \pm 109)$ ,  $(\pm 78, \pm 19)$ ,  $(\pm 78, \pm 59)$ ,  $(\pm 78, \mp 61)$ ,  $(\pm 78, \mp 101)$ . Подробного доказательства мы ради краткости не даем, так как для дальнейшего оно не является особенно необходимым.

VIII. Наконец, заметим, что если  $D$  — определитель двух эквивалентных форм  $(a, b, c)$ ,  $(a', b', c')$ ,  $M$  — их характеристическое число, и первая переходит во вторую при подстановке  $\alpha, \beta, \gamma, \delta$ , то при этом из каждого значения выражения  $\sqrt{M(a, b, c)}$ , например, из  $(g, h)$ , получается значение выражения  $\sqrt{M(a', b', c')}$ , именно,  $(\alpha g + \gamma h, \beta g + \delta h)$ . Доказательство каждый может провести без труда.

## О композиции форм

234

После того как мы предпослали все это о разбиении форм на классы, роды и порядки и изложили общие свойства, которые непосредственно получаются из этих подразделений, мы переходим теперь к другому, очень важному и до сих пор еще никем не затрагивавшемуся вопросу, именно, к *композиции форм*. В начале этого исследования мы, чтобы не прерывать в дальнейшем сплошного ряда доказательств, сразу же дадим следующую лемму.

**Лемма.** *Если имеется четыре ряда целых чисел:*

$$\begin{aligned} a, a', a'', \dots, a^{(n)}; b, b', b'', \dots, b^{(n)}; \\ c, c', c'', \dots, c^{(n)}; d, d', d'', \dots, d^{(n)}, \end{aligned}$$

*которые состоят из одинакового количества (именно, из  $n + 1$ ) членов и обладают тем свойством, что*

$$cd' - dc', cd'' - dc'', \dots, c'd'' - d'c'', \dots,$$

соответственно равны

$$k(ab' - ba'), k(ab'' - ba''), \dots, k(a'b'' - b'a''), \dots,$$

или что вообще

$$c^{(\lambda)}d^{(\mu)} - d^{(\lambda)}c^{(\mu)} = k(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}),$$

где  $k$  есть заданное целое число, и  $\lambda, \mu$  — какие-нибудь различные между собой целые числа между 0 и  $n$  включительно, большее из которых пусть  $\mu^*$ , и, кроме того, все  $a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}$  не имеют общего делителя, то могут быть найдены четыре таких целых числа  $\alpha, \beta, \gamma, \delta$ , что

$$\begin{aligned} \alpha a + \beta b &= c, \quad \alpha a' + \beta b' = c', \quad \alpha a'' + \beta b'' = c'', \dots, \\ \gamma a + \delta b &= d, \quad \gamma a' + \delta b' = d', \quad \gamma a'' + \delta b'' = d'', \dots, \end{aligned}$$

или вообще

$$\alpha a^{(\nu)} + \beta b^{(\nu)} = c^{(\nu)}, \quad \gamma a^{(\nu)} + \delta b^{(\nu)} = d^{(\nu)}.$$

Если это сделано, то

$$\alpha\delta - \beta\gamma = k.$$

Так как по предположению числа  $ab' - ba', ab'' - ba'', \dots, a'b'' - b'a'', \dots$  (количество которых равно  $n(n+1)/2$ ) не имеют общих делителей, то может быть найдено столько же других целых чисел, таких, что если первые перемножить с соответствующими вторыми, то сумма произведений будет равна 1 (п. 40). Эти множители будут обозначаться через  $(0, 1), (0, 2), \dots, (1, 2), \dots$ , вообще множитель числа  $a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}$  — через  $(\lambda, \mu)$ , так что

$$\sum (\lambda, \mu) (a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}) = 1.$$

(Знаком  $\sum$  мы обозначаем сумму всех значений последующего выражения, которые получаются, если  $\lambda, \mu$  придавать все раз-

---

\* При этом  $a$  рассматривается как  $a^{(0)}$  и  $b$  — как  $b^{(0)}$ . Отметим, что такое же равенство, очевидно, выполняется, если  $\lambda = \mu$  или  $\lambda > \mu$ .

личные значения между 0 и  $n$ , для которых  $\mu > \lambda$ .) Если положить затем

$$\begin{aligned} \sum (\lambda, \mu) (c^{(\lambda)} b^{(\mu)} - b^{(\lambda)} c^{(\mu)}) &= \alpha, & \sum (\lambda, \mu) (a^{(\lambda)} c^{(\mu)} - c^{(\lambda)} a^{(\mu)}) &= \beta, \\ \sum (\lambda, \mu) (d^{(\lambda)} b^{(\mu)} - b^{(\lambda)} d^{(\mu)}) &= \gamma, & \sum (\lambda, \mu) (a^{(\lambda)} d^{(\mu)} - d^{(\lambda)} a^{(\mu)}) &= \delta, \end{aligned}$$

то эти числа  $\alpha, \beta, \gamma, \delta$  будут обладать требуемыми свойствами.

**Доказательство. I.** Если  $\nu$  обозначает какое-нибудь целое число между 0 и  $n$ , то

$$\begin{aligned} \alpha a^{(\nu)} + \beta b^{(\nu)} &= \sum (\lambda, \mu) (c^{(\lambda)} b^{(\mu)} a^{(\nu)} - b^{(\lambda)} c^{(\mu)} a^{(\nu)} + a^{(\lambda)} c^{(\mu)} b^{(\nu)} - c^{(\lambda)} a^{(\mu)} b^{(\nu)}) = \\ &= \frac{1}{k} \sum (\lambda, \mu) (c^{(\lambda)} d^{(\mu)} c^{(\nu)} - d^{(\lambda)} c^{(\mu)} c^{(\nu)}) = \\ &= \frac{1}{k} c^{(\nu)} \sum (\lambda, \mu) (c^{(\lambda)} d^{(\mu)} - d^{(\lambda)} c^{(\mu)}) = \\ &= c^{(\nu)} \sum (\lambda, \mu) (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}) = \\ &= c^{(\nu)}. \end{aligned}$$

Аналогичным подсчетом находим

$$\gamma a^{(\nu)} + \delta b^{(\nu)} = d^{(\nu)}.$$

**II.** Так как тем самым

$$c^{(\lambda)} = \alpha a^{(\lambda)} + \beta b^{(\lambda)}, \quad c^{(\mu)} = \alpha a^{(\mu)} + \beta b^{(\mu)},$$

то

$$c^{(\lambda)} b^{(\mu)} - b^{(\lambda)} c^{(\mu)} = \alpha (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}),$$

и аналогично

$$\begin{aligned} a^{(\lambda)} c^{(\mu)} - c^{(\lambda)} a^{(\mu)} &= \beta (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}), \\ d^{(\lambda)} b^{(\mu)} - b^{(\lambda)} d^{(\mu)} &= \gamma (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}), \\ a^{(\lambda)} d^{(\mu)} - d^{(\lambda)} a^{(\mu)} &= \delta (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}), \end{aligned}$$

и из этих формул значения  $\alpha, \beta, \gamma, \delta$  могут быть найдены намного легче, если только числа  $\lambda, \mu$  взяты такими, что  $a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}$  не равно нулю, что заведомо возможно, так как по условию у всех чисел  $a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}$  нет общих делителей, и потому все они одновременно не могут быть равны 0. Из этих равенств



получается, если первое перемножить с четвертым, а второе с третьим и вычесть, что

$$\begin{aligned} (\alpha\delta - \beta\gamma) (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)})^2 = \\ = (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)}) (c^{(\lambda)} d^{(\mu)} - d^{(\lambda)} c^{(\mu)}) = k (a^{(\lambda)} b^{(\mu)} - b^{(\lambda)} a^{(\mu)})^2, \end{aligned}$$

и потому обязательно

$$\alpha\delta - \beta\gamma = k.$$

235

Если форма

$$AX^2 + 2BXY + CY^2 = F$$

переходит в произведение двух форм

$$ax^2 + 2bxy + cy^2 = f, \quad a'x'^2 + 2b'x'y' + c'y'^2 = f'$$

при подстановке вида

$$\begin{aligned} X &= rxx' + p'xy' + p''yx' + p'''yy', \\ Y &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned}$$

(что мы для краткости всегда в дальнейшем будем выражать так: если  $F$  переходит в  $ff'$  при подстановке  $r, p', p'', p'''; q, q', q'', q'''$ )\*, то мы будем говорить просто, что *форма  $F$  преобразуема в  $ff'$*  если, кроме того, это преобразование таково, что шесть чисел  $pq' - qr', pq'' - qr'', pq''' - qr''', p'q'' - q'r'', p'q''' - q'r''', p''q''' - q''r'''$  не имеют общих делителей, то мы будем называть форму  $F$  *составленной (скомпонированной) из форм  $f, f'$* .

Мы начнем наше исследование с самого общего предположения, именно, что  $F$  переходит в  $ff'$  при подстановке  $r, p', p'', p'''; q, q', q'', q'''$ , и посмотрим, что отсюда следует. Очевидно, что этому предположению будут полностью эквивалентны следующие девять

---

\* Таким образом, при этом обозначении принимается во внимание порядок расположения коэффициентов  $r, p', \dots$  и форм  $f, f'$ . Но легко видеть, что если изменить порядок расположения форм  $f, f'$  на обратный, то коэффициенты  $p', q'$  поменяются местами с  $p'', q''$ , а все остальные коэффициенты останутся на месте.

равенств (т. е. если эти равенства имеют место, то при названной подстановке  $F$  будет переходить в  $ff'$ , и обратно):

$$\begin{aligned}
 [1] \quad & Ap^2 + 2Bpq + Cq^2 = aa', \\
 [2] \quad & Ap'^2 + 2Bp'q' + Cq'^2 = ac', \\
 [3] \quad & Ap''^2 + 2Bp''q'' + Cq''^2 = ca', \\
 [4] \quad & Ap'''^2 + 2Bp'''q''' + Cq'''^2 = cc', \\
 [5] \quad & App' + B(pq' + qp') + Cqq' = ab', \\
 [6] \quad & App'' + B(pq'' + qp'') + Cqq'' = ba', \\
 [7] \quad & Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc', \\
 [8] \quad & Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb', \\
 [9] \quad & A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb',
 \end{aligned}$$

Пусть определители форм  $F, f, f'$  соответственно равны  $D, d, d'$ , наибольшие общие делители чисел  $A, 2B, C; a, 2b, c; a', 2b', c'$  — соответственно  $M, m, m'$  (которые мы будем предполагать взятыми положительными); далее, определим шесть таких целых чисел  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ , что

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \quad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m';$$

наконец, обозначим числа

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''', \quad p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

соответственно через  $P, Q, R, S, T, U$ , а их наибольший общий делитель, взятый положительным, — через  $k$ . Если положить тогда

$$[10] \quad App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta,$$

то, согласно равенству [9], будет

$$[11] \quad Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta.$$

Из этих одиннадцати равенств (с [1] по [11]) мы выводим следующие новые равенства \*:

$$\begin{aligned}
 [12] \quad & DP^2 = d'a^2, \\
 [13] \quad & DP(R - S) = 2d'ab, \\
 [14] \quad & DPU = d'ac - (\Delta^2 - dd'), \\
 [15] \quad & D(R - S)^2 = 4d'b^2 + 2(\Delta^2 - dd'), \\
 [16] \quad & D(R - S)U = 2d'bc, \\
 [17] \quad & DU^2 = d'c^2, \\
 [18] \quad & DQ^2 = da'^2, \\
 [19] \quad & DQ(R + S) = 2da'b', \\
 [20] \quad & DQT = da'c' - (\Delta^2 - dd'), \\
 [21] \quad & D(R + S)^2 = 4db'^2 + 2(\Delta^2 - dd'), \\
 [22] \quad & D(R + S)T = 2db'c', \\
 [23] \quad & DT^2 = dc'^2.
 \end{aligned}$$

Из них снова получаются следующие два:

$$\begin{aligned}
 0 &= 2d'a^2(\Delta^2 - dd'), \\
 0 &= (\Delta^2 - dd')^2 - 2d'ac(\Delta^2 - dd'),
 \end{aligned}$$

именно, первое из [12]·[15] — [13]·[13], а второе из [14]·[14] — [12]·[17], а отсюда легко увидеть, что обязательно  $\Delta^2 - dd' = 0$ , независимо от того, равно нулю  $a$  или нет \*\*. Мы предположим поэтому, что в правых частях равенств [14], [15], [20], [21] выражение  $\Delta^2 - dd'$  равно нулю.

Если положить теперь

---

\* Эти равенства получаются так: [12] из  $[5]^2 - [1] \cdot [2]$ ; [13] из  $[5] \cdot [9] - [1] \cdot [7] - [2] \cdot [6]$ ; [14] из  $[10] \cdot [11] - [6] \cdot [7]$ ; [15] из  $[5] \cdot [8] + [5] \cdot [8] + [10]^2 - [11]^2 - [1] \cdot [4] - [2] \cdot [3] - [6] \cdot [7] - [6] \cdot [7]$ ; [16] из  $[8] \cdot [9] - [3] \cdot [7] - [4] \cdot [6]$ ; [17] из  $[8]^2 - [3] \cdot [4]$ . Вывод остальных шести равенств получается таким же образом, если только поменять местами равенства [2], [5], [7] соответственно с [3], [6], [8], а остальные равенства [1], [4], [9], [10], [11] оставить на месте, именно, [18] получается из  $[6]^2 - [1] \cdot [3]$  и т. д.

\*\* Этот вывод равенства  $\Delta^2 = dd'$  достаточен для нашей цели; мы могли бы указать более изящный, но слишком длинный способ для вывода равенства  $0 = (\Delta^2 - dd')^2$  непосредственно из равенств [1] — [11].

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn',$$

$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n$$

(причем нужно заметить, что  $n, n'$  могут быть и дробными, хотя  $mn', m'n$  обязательно целые), то из равенств с [12] по [17] легко получается, что

$$Dm^2n'^2 = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'm^2,$$

и аналогично из равенств с [18] по [23] —

$$Dm'^2n^2 = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'^2.$$

Поэтому  $d = Dn^2, d' = Dn'^2$ , откуда мы получаем в качестве **первого следствия**: *определители форм  $F, f, f'$  обязательно относятся один к другому как квадраты*, — и в качестве **второго следствия**:  *$D$  всегда входит в числа  $dm'^2, d'm^2$* . Отсюда вытекает, что  $D, d, d'$  имеют одинаковые знаки, и что в произведение  $ff'$  не преобразуема никакая форма, определитель которой больше, чем наибольший общий делитель чисел  $dm'^2, d'm^2$ ,

Если умножить равенства [12], [13], [14], а также равенства [13], [15], [16] и [14], [16], [17] соответственно на  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ , сложить каждый раз три произведения, суммы разделить на  $Dmn'$ , и написать  $Dn'^2$  вместо  $d'$ , то мы получим

$$P = an', R - S = 2bn'. U = cn'.$$

Аналогичным образом получается, если равенства [18], [19], [20], далее [19], [21], [22] и [20], [22], [23] умножить соответственно на  $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ , то

$$Q = a'n, R + S = 2b'n, T = c'n.$$

Отсюда получается в качестве **третьего следствия**: *числа  $a, 2b, c$  пропорциональны числам  $P, R - S, U$ , и если отношение первых ко вторым положить равным  $1:n'$ , то  $n'$  есть квадратный корень из  $d'/D$ ; точно так же числа  $a', 2b', c'$  имеют одинаковые отношения к  $Q, R + S, T$ , и если положить их равными  $1:n$ , то  $n$  есть квадратный корень из  $d/D$ .*

Величины  $n, n'$  могут быть как положительными, так и отрицательными квадратными корнями из  $d/D, d'/D$ , на чем мы

будем основывать одно различие, которое на первый взгляд кажется бесцельным, но польза которого в дальнейшем станет ясной. Именно. мы будем говорить, что при преобразовании формы  $F$  в  $ff'$  форма  $f$  берется прямо, если  $n$  положительно, и обратно, если  $n$  отрицательно, и аналогично  $f'$  берется прямо или обратно в зависимости от того, положительно  $n'$  или отрицательно. Если же добавляется еще условие, что  $k = 1$ , то форма  $F$  называется составленной или из обеих форм  $f, f'$  прямо, или из обеих обратно, или из  $f$  прямо, а из  $f'$  обратно, или из  $f$  обратно, а из  $f'$  прямо, в зависимости от того, положительны ли оба числа  $n, n'$ , или оба отрицательны, или первое положительно, а второе отрицательно, или первое отрицательно, а второе положительно. Впрочем, каждый может легко убедиться, что эти отношения не зависят от порядка, в котором следуют формы  $f, f'$  (ср. первое замечание \* к этому пункту).

Далее заметим, что наибольший общий делитель чисел  $P, Q, R, S, T, U$ , именно,  $k$ , входит в числа  $mn', m'n$  (как это вытекает из выведенных выше для этих чисел значений), и потому квадрат числа  $k$  входит в  $m^2n'^2, m'^2n^2$ , и  $Dk^2$  — в  $d'm^2, dm'^2$ . Но и обратно, каждый общий делитель чисел  $mn', m'n$  будет входить в  $k$ . Действительно, пусть  $e$  — такой делитель, который, очевидно, будет входить также в числа  $an', 2bn', cn', a'n, 2b'n, c'n$ , т. е. также в числа  $P, R - S, U, Q, R + S, T$  и, следовательно, также в  $2R$  и  $2S$ . Если бы теперь число  $2R/e$  было нечетным, то должно было бы быть нечетным и число  $2S/e$  (так как сумма и разность являются четными числами), и тем самым было бы нечетным и их произведение. Но это произведение равно  $\frac{4}{e^2} (b'^2n^2 - b^2n'^2) = \frac{4}{e^2} (d'n^2 + a'c'n^2 - dn'^2 - acn'^2) = \frac{4}{e^2} (a'c'n^2 - acn'^2)$ , и поэтому четно, так как  $e$  входит в  $a'n, c'n, an', cn'$ . Поэтому  $2R/e$  обязательно четно, и потому  $R$ , а также и  $S$  делятся на  $e$ . Так как тем самым  $e$  входит во все шесть чисел  $P, Q, R, S, T, U$ , то оно будет входить также и в их наибольший общий делитель  $k$ . Отсюда следует, что  $k$  есть наибольший общий делитель чисел  $mn', m'n$ , откуда легко видеть, что  $Dk^2$  есть наибольший общий делитель чисел  $dm'^2$ ,

\* Стр. 298. — Прим. ред.

$d'm^2$ . Это четвертое следствие. Очевидно, таким образом, что если форма  $F$  составлена из  $f$  и  $f'$ , то  $D$  будет наибольшим общим делителем чисел  $dm'^2$  и  $d'm^2$ , и обратно, и это свойство может быть взято также за определение составленной формы. Форма, составленная из форм  $f, f'$ , имеет поэтому наибольший определитель среди всех форм, которые преобразуемы в произведение  $ff'$ .

Прежде чем мы сможем продолжать дальше, мы должны сначала точнее определить значение  $\Delta$ , которое, как мы показали, равно  $\sqrt{dd'} = \sqrt{D^2 n^2 n'^2}$ , но знак которого до сих пор еще не был определен. Для этой цели мы из основных равенств с [1] по [11] выведем равенство  $DPQ = \Delta aa'$  (которое получается из [5]·[6] — [1]·[11]), и тем самым  $Daa'nn' = \Delta aa'$ , откуда, если ни одно из чисел  $a, a'$  не равно нулю, следует  $\Delta = Dnn'$ . Но точно таким же образом из основных равенств могут быть выведены восемь других равенств, у которых слева будет  $Dnn'$ , а справа  $\Delta$ , умноженное на  $2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc'$ \*, откуда, поскольку ни все  $a, 2b, c$ , ни все  $a', 2b', c'$ , не могут быть равны 0, легко получается, что во всех случаях  $\Delta = Dnn'$ , и потому  $\Delta$  имеет тот же знак, что и  $D, d, d'$ , или противоположный в зависимости от того, имеют ли  $n, n'$  одинаковые или противоположные знаки.

Далее, заметим, что числа  $aa', 2ab', ac', 2ba', 4bb', 2bc', ca', 2cb', cc', 2bb' + 2\Delta, 2bb' - 2\Delta$  все делятся на  $mm'$ . Для девяти первых это ясно само собой, а для двух остальных может быть доказано подобно тому, как выше показывалось, что  $R$  и  $S$  делятся на  $e$ . Именно, очевидно, что  $4bb' + 4\Delta$  и  $4bb' - 4\Delta$  делятся на  $mm'$  (так как  $4\Delta = \sqrt{16dd'}$  и  $4d$  делится на  $m^2$ ,  $4d'$  — на  $m'^2$ , и тем самым  $16dd'$  делится на  $m^2 m'^2$  и  $4\Delta$  — на  $mm'$ ), и разность частных есть четное число; но легко показать, что произведение частных тоже четно, откуда следует, что каждое из этих частных четно, и как  $2bb' + 2\Delta$ , так и  $2bb' - 2\Delta$  делятся на  $mm'$ .

Из одиннадцати основных равенств теперь легко выводятся следующие шесть равенств:

$$AP^2 = aa'q'^2 - 2ab'qq' + ac'q^2,$$

---

\* Вывод, который читатель легко может найти сам, мы здесь ради краткости должны опустить.

$$\begin{aligned}
AQ^2 &= aa'q''^2 - 2ba'qq'' + ca'q^2, \\
AR^2 &= aa'q'''^2 - 2(bb' + \Delta)qq''' + cc'q^2, \\
AS^2 &= ac'q''^2 - 2(bb' - \Delta)q'q'' + ca'q'^2, \\
AT^2 &= ac'q'''^2 - 2bc'q'q''' + cc'q'^2, \\
AU^2 &= ca'q'''^2 - 2cb'q''q''' + cc'q''^2.
\end{aligned}$$

Поэтому все величины  $AP^2$ ,  $AQ^2$ , ... делятся на  $mm'$ , откуда, так как  $k^2$  есть наибольший общий делитель чисел  $P^2$ ,  $Q^2$ ,  $R^2$ , ..., легко следует, что и  $Ak^2$  делится на  $mm'$ . Если же вместо  $a$ ,  $2b$ ,  $c$ ,  $a'$ ,  $2b'$ ,  $c'$  подставить их значения  $P/n'$ , ... или  $(pq' - qp')/n'$ , ..., то эти равенства перейдут в шесть других, у которых справа будут стоять произведения величины  $(q'q'' - qq''')/nn'$  и чисел  $P^2$ ,  $Q^2$ ,  $R^2$ , ... Очень простую выкладку мы предоставляем читателю. Отсюда (так как не могут быть одновременно равны 0 все величины  $P^2$ ,  $Q^2$ , ...) получается  $Ann' = q'q'' - qq'''$ .

Аналогичным образом из основных равенств выводятся шесть других равенств, которые отличаются от предыдущих только тем, что вместо  $A$  всюду стоит  $C$ , а вместо  $q$ ,  $q'$ ,  $q''$ ,  $q'''$  соответственно  $p$ ,  $p'$ ,  $p''$ ,  $p'''$ , и которые мы ради краткости не выписываем. Из них таким же образом следует, что  $Ck^2$  делится на  $mm'$ , и  $Cnn' = p'p'' - pp'''$ .

Наконец, из того же источника вытекают следующие шесть равенств:

$$\begin{aligned}
BP^2 &= -aa'p'q' + ab'(pq' + qp') - ac'pq, \\
BQ^2 &= -aa'p''q'' + ba'(pq'' + qp'') - ca'pq, \\
BR^2 &= -aa'p'''q''' + (bb' + \Delta)(pq''' + q'p''') - cc'pq, \\
BS^2 &= -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q'; \\
BT^2 &= -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q', \\
BU^2 &= -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q'',
\end{aligned}$$

из которых так же, как и раньше, следует, что  $2Bk^2$  делится на  $mm'$ , и  $2Bnn' = pq''' + qp''' - p'q'' - q'p''$ .

Так как теперь  $Ak^2$ ,  $2Bk^2$ ,  $Ck^2$  делятся на  $mm'$ , то легко видеть, что и  $Mk^2$  должно делиться на  $mm'$ . Но из основных равенств получается, что  $M$  входит в  $aa'$ ,  $2ab'$ ,  $ac'$ ,  $2ba'$ ,  $4bb'$ ,  $2bc'$ ,  $ca'$ ,  $2cb'$ ,  $cc'$  и потому также в  $am'$ ,  $2bm'$ ,  $cm'$  (которые являются наибольшими общими делителями соответственно трех первых, трех средних

и трех последних из этих девяти чисел), и, наконец, и в произведение  $mm'$ , которое есть наибольший общий делитель этих последних трех величин. Поэтому в том случае, когда  $F$  составлена из форм  $f, f'$ , т. е.  $k = 1$ , обязательно должно, очевидно, быть  $M = mm'$ . Это — пятое следствие.

Если наибольший общий делитель чисел  $A, B, C$  равен  $\mathfrak{M}$ , то он или равен  $M$  (в случае, когда форма  $F$  собственно примитивна или произведена из собственно примитивной формы), или равен  $M/2$  (в случае, когда форма  $F$  несобственно примитивна или произведена из несобственно примитивной формы). Если, аналогично, обозначить наибольшие общие делители чисел  $a, b, c; a', b', c'$  соответственно через  $m, m'$ , то  $m$  или  $=m$ , или  $=m/2$ , и  $m'$  или  $=m'$ , или  $=m'/2$ . Но теперь, очевидно,  $m^2$  входит в  $d$ ,  $m'^2$  — в  $d'$ , и потому  $m^2m'^2$  входит в  $dd'$  или  $\Delta^2$  и  $mm'$  — в  $\Delta$ . Поэтому из шести последних равенств для  $BP^2, \dots$  следует, что  $mm'$  входит в  $Bk^2$ , и потому (так как оно входит и в  $Ak^2$  и  $Ck^2$ ) также и в  $\mathfrak{M}k^2$ . Следовательно, если  $F$  составлена из  $f, f'$ , то  $mm'$  входит в  $\mathfrak{M}$ . Если поэтому в этом случае каждая из форм  $f, f'$  собственно примитивна или произведена из собственно примитивной формы, или если  $mm' = mm' = M$ , то будет  $\mathfrak{M} = M$ , т. е.  $F$  тоже будет формой этого же типа. Если же при тех же предположениях или каждая из форм  $f, f'$ , или по крайней мере одна из них, например,  $f$ , несобственно примитивна или произведена из несобственно примитивной формы, то из основных равенств следует, что  $aa', 2ab', ac', ba', 2bb', bc', ca', 2cb', cc'$  и тем самым также  $am', bm', cm'$ , а, значит, и  $mm' = \frac{1}{2} mm' = \frac{1}{2} M$  делятся на  $\mathfrak{M}$ . Следовательно, в этом случае обязательно  $\mathfrak{M} = \frac{1}{2} M$ , т. е. и форма  $F$  или несобственно примитивна, или произведена из несобственно примитивной формы. Это представляет собой шестое следствие.

Наконец, заметим, что если не рассматривать  $n, n'$  как неизвестные, ни одно из которых не равно 0 (как это мы делали раньше), а предполагать выполнение девяти равенств

$$\begin{aligned} an' &= P, & 2bn' &= R - S, & cn' &= U, \\ a'n &= Q, & 2b'n &= R + S, & c'n &= T, \end{aligned}$$



$Ann' = q'q'' - qq'''$ ,  $2Bnn' = pq''' + qp''' - p'q'' - q'p''$ ,  $Cnn' = p'p'' - pp'''$  (которые, так как нам часто придется на них ссылаться, мы обозначим через  $\Omega$ ), то подстановкой легко может быть установлено, что обязательно выполняются и основные равенства с [1] по [9], или что форма  $(A, B, C)$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$  переходит в произведение форм  $(a, b, c)$ ,  $(a', b', c')$ , и что, кроме того,

$$b^2 - ac = n^2(B^2 - AC), \quad b'^2 - a'c' = n'^2(B^2 - AC).$$

Вычисления, приводить которые здесь было бы слишком длинно мы предоставляем усердию читателя.

### 236

**Задача.** Пусть даны две формы, определители которых или равны, ли по крайней мере относятся один к другому как квадраты двух чисел; найти составленную из них форму.

**Решение.** Пусть  $(a, b, c) = f$ ,  $(a', b', c') = f'$  — композируемые формы,  $d, d'$  — их определители, наибольшие общие делители чисел  $a, 2b, c$ ;  $a', 2b', c'$  равны соответственно  $m, m'$ , и наибольший общий делитель чисел  $dm'^2, d'm^2$ , взятый с тем же знаком, что и  $d, d'$ , равен  $D$ . Тогда  $dm'^2/D, d'm^2/D$  будут взаимно простыми положительными числами, а их произведение будет квадратом; поэтому и сами они квадраты (п. 21). Следовательно,  $\sqrt{d/D}$  и  $\sqrt{d'/D}$  — рациональные числа, которые мы положим равными  $n, n'$ , причем мы будем брать для  $n$  положительный или отрицательный знак в зависимости от того, должна ли форма  $f$  входить в композицию прямо или обратно, и точно так же знак  $n'$  мы будем определять в зависимости от того, как должна входить в композицию форма  $f'$ . Поэтому  $mn', m'n$  будут целыми взаимно простыми числами, в то время как  $n, n'$  могут быть и дробными. После того, как это сделано, заметим, что числа  $an', cn', a'n, c'n, bn' + b'n, bn' - b'n$  целые; в отношении первых четырех это ясно само собой (так как  $an' = \frac{a}{m}mn'$  и т. д.), в отношении же двух остальных это доказывается таким же образом, как выше в предыдущем

пункте показывалось, что  $R$  и  $S$  делятся на  $e$ . Возьмем теперь четыре произвольных целых числа  $\Omega, \Omega', \Omega'', \Omega'''$ , с одним только условием, чтобы в следующих равенствах (I) четыре стоящие слева величины не были все равны 0 одновременно, и положим

$$(I) \quad \begin{cases} \Omega' an' + \Omega'' a'n + \Omega''' (bn' + b'n) = \mu q, \\ -\Omega an' + \Omega''' c'n - \Omega'' (bn' - b'n) = \mu q', \\ \Omega''' cn' - \Omega a'n + \Omega' (bn' - b'n) = \mu q'', \\ -\Omega'' cn' - \Omega' c'n - \Omega (bn' + b'n) = \mu q''', \end{cases}$$

так что  $q, q', q'', q'''$  будут целыми числами, которые не имеют общих делителей, что достигается, если за  $\mu$  взять наибольший общий делитель четырех чисел, которые в этих равенствах стоят слева. Тогда, согласно п. 40, могут быть найдены четыре таких целых числа  $\wp, \wp', \wp'', \wp'''$ , что

$$\wp q + \wp' q' + \wp'' q'' + \wp''' q''' = 1.$$

Если это сделано, то определим четыре числа  $p, p', p'', p'''$  следующими равенствами:

$$(II) \quad \begin{cases} \wp' an' + \wp'' a'n + \wp''' (bn' + b'n) = p, \\ -\wp an' + \wp''' c'n - \wp'' (bn' - b'n) = p', \\ \wp''' cn' - \wp a'n + \wp' (bn' - b'n) = p'', \\ -\wp'' cn' - \wp' c'n - \wp (bn' + b'n) = p'''. \end{cases}$$

Наконец, положим

$$\begin{aligned} q'q'' - qq''' &= Ann', & pq''' + qp''' - p'q'' - q'p'' &= 2Bnn', \\ p'p'' - pp''' &= Cnn'. \end{aligned}$$

Тогда числа  $A, B, C$  будут целыми, и форма  $(A, B, C) = F$  будет составлена из форм  $f, f'$ .

**Доказательство.** I. Из равенств (I) без труда получаются следующие четыре равенства:

$$(III) \quad \begin{cases} 0 = q'cn' - q''c'n - q''' (bn' - b'n), \\ 0 = qcn' + q'''a'n - q'' (bn' + b'n), \\ 0 = q'''an' + qc'n - q' (bn' + b'n), \\ 0 = q''an' - q'a'n - q (bn' - b'n). \end{cases}$$

II. Если мы теперь предположим, что целые числа  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$ ,  $\mathfrak{A}'$ ,  $\mathfrak{B}'$ ,  $\mathfrak{C}'$ ,  $\mathfrak{N}$ ,  $\mathfrak{N}'$  определены так, что

$$\begin{aligned}\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m, \\ \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m', \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1,\end{aligned}$$

то будет

$$\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1.$$

Отсюда при помощи равенств (III) легко устанавливается, что если положить

$$\begin{aligned}-q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= q, \\ q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= q', \\ -q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}'\mathfrak{N}' - \mathfrak{B}\mathfrak{N}) &= q'', \\ q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= q''',\end{aligned}$$

то имеют место равенства

$$(IV) \quad \begin{cases} q'an' + q''a'n + q'''(bn' + b'n) = q, \\ -qan' + q'''c'n - q''(bn' - b'n) = q', \\ q'''cn' - qa'n + q'(bn' - b'n) = q'', \\ -q''cn' - q'c'n - q(bn' + b'n) = q'''. \end{cases}$$

Если  $\mu = 1$ , то эти равенства не являются необходимыми, а вместо них могут быть использованы равенства (I), которым они вполне аналогичны. Если теперь из равенств (II), (IV) найдены значения  $A\mathfrak{N}\mathfrak{N}'$ ,  $2B\mathfrak{N}\mathfrak{N}'$ ,  $C\mathfrak{N}\mathfrak{N}'$  (т. е. числа  $q'q'' - qq'''$ , ...), и то, что взаимно уничтожается, отброшено, то оказывается, что останутся слагаемые, являющиеся или произведениями целых чисел на  $\mathfrak{N}\mathfrak{N}'$ , или произведениями целых чисел на  $d\mathfrak{N}'^2$ , или произведениями целых чисел на  $d'n^2$ , и что кроме того, все слагаемые  $2B\mathfrak{N}\mathfrak{N}'$  будут содержать сомножитель 2. Отсюда мы выводим (так как  $d\mathfrak{N}'^2 = d'n^2$  и тем самым  $\frac{d\mathfrak{N}'^2}{\mathfrak{N}\mathfrak{N}'} = \frac{d'n^2}{\mathfrak{N}\mathfrak{N}'} = \sqrt{dd'}$  являются целыми числами), что числа  $A$ ,  $B$ ,  $C$  целые.

III. Если подставить значения  $p, p', p'', p'''$  из равенств (II), то при помощи равенств (III) и равенства

$$\wp q + \wp' q' + \wp'' q'' + \wp''' q''' = 1$$

легко установить, что

$$\begin{aligned} pq' - qp' &= an', & pq''' - qp''' - p'q'' + q'p'' &= 2bn', & p''q''' - q''p''' &= cn', \\ pq'' - qp'' &= a'n, & pq''' - qp''' + p'q'' - q'p'' &= 2b'n, & p'q''' - q'p''' &= c'n, \end{aligned}$$

и эти равенства совпадают с первыми шестью из равенств  $\Omega$  в предыдущем пункте; остальные же три имеют место уже по предположению. Поэтому (ср. заключение предыдущего пункта) форма  $F$  переходит при подстановке  $p, p', p'', p'''; q, q', q'', q'''$  в  $ff'$ , и определитель ее равен  $D$ , т. е. наибольшему общему делителю чисел  $dm'^2, d'm^2$ ; поэтому, в силу четвертого следствия предыдущего пункта, форма  $F$  составлена из  $f$  и  $f'$ . Наконец, легко видеть, что  $F$  составлена из  $f, f'$  так, как предписывалось, так как знаки чисел  $n, n'$  правильно определены уже сначала.

### 237

**Теорема.** Если форма  $F$  преобразуема в произведение двух форм  $f, f'$  и форма  $f'$  содержит форму  $f''$ , то  $F$  преобразуема также в произведение форм  $f, f''$ .

**Доказательство.** Сохраним для форм  $F, f, f'$  все обозначения п. 235, и пусть форма  $f''$  равна  $(a'', b'', c'')$ , и форма  $f'$  переходит в  $f''$  при подстановке  $\alpha, \beta, \gamma, \delta$ .

Тогда без труда видно, что  $F$  переходит в  $ff''$  при подстановке

$$\begin{aligned} \alpha p + \gamma p', \beta p + \delta p', \alpha p'' + \gamma p''', \beta p'' + \delta p'''; \\ \alpha q + \gamma q', \beta q + \delta q', \alpha q'' + \gamma q''', \beta q'' + \delta q''', \end{aligned}$$

что и требовалось доказать.

Если для краткости обозначить коэффициенты  $\alpha p + \gamma p', \beta p + \delta p', \dots$  соответственно через  $\wp, \wp', \wp'', \wp'''; \Omega, \Omega', \Omega'', \Omega'''$ , и число  $\alpha\delta - \beta\gamma$  — через  $e$ , то из равенств  $\Omega$  п. 235 легко устанавливаются равенства

$$\begin{aligned} \wp\Omega' - \Omega\wp' &= an'e, \\ \wp\Omega''' - \Omega\wp''' - \wp'\Omega'' + \Omega'\wp'' &= 2bn'e, \end{aligned}$$

$$\begin{aligned}
\mathfrak{P}''\Omega''' - \Omega''\mathfrak{P}''' &= cn'e, \\
\mathfrak{P}\Omega'' - \Omega\mathfrak{P}'' &= \alpha^2 a'n + 2\alpha\gamma b'n + \gamma^2 c'n = a''n, \\
\mathfrak{P}\Omega''' - \Omega\mathfrak{P}''' + \mathfrak{P}'\Omega'' - \Omega'\mathfrak{P}'' &= 2b''n, \\
\mathfrak{P}'\Omega''' - \Omega'\mathfrak{P}''' &= c''n, \\
\Omega'\Omega'' - \Omega\Omega''' &= Ann'e, \\
\mathfrak{P}\Omega''' + \Omega\mathfrak{P}''' - \mathfrak{P}'\Omega'' - \Omega'\mathfrak{P}'' &= 2Bnn'e, \\
\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e.
\end{aligned}$$

Если теперь обозначить определитель формы  $f''$  через  $d''$ , то  $e$  будет квадратным корнем из  $d''/d'$ , причем положительным или отрицательным в зависимости от того, содержит ли форма  $f'$  форму  $f''$  собственно или несобственно.

Поэтому  $n'e$  есть квадратный корень из  $d''/D$ , откуда вытекает, что девять предыдущих равенств полностью аналогичны равенствам  $\Omega$  п. 235, и что при преобразовании формы  $F$  в  $ff''$  форма  $f$  берется так же, как при преобразовании формы  $F$  в  $ff'$ , а форма  $f''$  берется или так же, как  $f'$ , или противоположным образом, в зависимости от того, содержит ли  $f'$  форму  $f''$  собственно или несобственно.

## 238

**Теорема.** Если форма  $F$  содержится в форме  $F'$  и преобразуема в произведение форм  $f, f'$ , то и форма  $F'$  преобразуема в это же произведение.

**Доказательство.** Если мы сохраним для форм  $F, f, f'$  те же обозначения, что и выше, и предположим, что форма  $F'$  переходит в  $F$  при подстановке  $\alpha, \beta, \gamma, \delta$ , то легко видеть, что  $F'$  при подстановке

$$\begin{aligned}
&\alpha p + \beta q, \quad \alpha p' + \beta q', \quad \alpha p'' + \beta q'', \quad \alpha p''' + \beta q'''; \\
&\gamma p + \delta q, \quad \gamma p' + \delta q', \quad \gamma p'' + \delta q'', \quad \gamma p''' + \delta q'''
\end{aligned}$$

превращается в то же самое, во что превращается  $F$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$ , т. е. что  $F'$  переходит при этой подстановке в  $ff'$ .

Кроме того, посредством вычислений, аналогичных вычислениям предыдущего пункта, легко устанавливается, что  $F'$  преобразуема в  $ff'$  таким же образом, что и  $F$ , если  $F'$  содержит форму  $F$  собственно, и что, напротив, если  $F$  содержится в  $F'$  несобственно,

то преобразования формы  $F$  в  $ff'$  и формы  $F'$  в  $ff'$  противоположны по отношению каждой из форм  $f, f'$ , т. е. что та из этих форм, которая в одно из преобразований входит прямо, в другом берется обратно.

Комбинируя настоящую теорему с теоремой предыдущего пункта, мы получаем следующую более общую теорему.

*Если форма  $F$  преобразуема в произведение  $ff'$ , и формы  $f, f'$  содержат соответственно формы  $g, g'$ , а форма  $F$  содержится в форме  $G$ , то  $G$  преобразуема в произведение  $gg'$ .*

Действительно, по теореме этого пункта  $G$  преобразуема в  $ff'$ , поэтому, по теореме предыдущего пункта, и в  $fg'$ , и, по той же теореме, — и в  $gg'$ . Далее ясно, что если все три формы  $f, f', G$  содержат формы  $g, g', F$  собственно, то  $G$  преобразуема в  $gg'$  таким же образом относительно  $g, g'$ , каким относительно  $f, f'$  преобразуема  $F$  в  $ff'$ ; что аналогично обстоит дело, если первые три формы содержат последние три несобственно; наконец, так же легко можно определить, как преобразуема  $G$  в  $gg'$ , если из трех форм  $f, f', G$  одна содержит соответствующую из трех форм  $g, g', F$  не так, как содержат соответствующие формы две другие.

Если формы  $F, f, f'$  эквивалентны формам  $G, g, g'$ , то последние будут иметь те же определители, что и первые, и то, что числа  $m, m'$  обозначают для форм  $f, f'$ , они будут обозначать и для форм  $g, g'$  (п. 161). Отсюда при помощи четвертого следствия п. 235 без труда выводится, что в этом случае  $G$  составлена из  $g, g'$ , если  $F$  составлена из  $f, f'$ , и что форма  $g$  входит в первую композицию таким же образом, как  $f$  — во вторую, если  $F$  эквивалентна форме  $G$  таким же образом, как  $f$  — форме  $g$ , и наоборот; и что подобно этому  $g'$  берется в первой композиции или таким же, или противоположным образом по сравнению с тем, как берется  $f'$  во второй композиции, в зависимости от того, является ли эквивалентность форм  $f', g'$  однотипной с эквивалентностью форм  $F, G$ , или нет.

**Теорема.** *Если форма  $F$  составлена из форм  $f, f'$ , то всякая другая форма, которая преобразуема таким же образом, что и  $F$ , в произведение  $ff'$ , будет собственно содержать форму  $F$ .*

**Доказательство.** Если сохранить для  $F, f, f'$  все обозначения п. 235, то равенства  $\Omega$  будут иметь место и здесь. Если предположить, что форма  $F' = (A', B', C')$ , определитель которой пусть равен  $D'$ , переходит в произведение  $ff'$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$ , и числа  $pq' - qp', pq'' - qp'', pq''' - qp''', p'q'' - q'p'', p'q''' - q'p''', p''q''' - q''p'''$  обозначить соответственно через

$$P', Q', R', S', T', U',$$

то получится девять равенств, совершенно аналогичных равенствам  $\Omega$ , именно:

$$P' = an', R' - S' = 2bn', U' = cn',$$

$$Q' = a'n, R' + S' = 2b'n, T' = c'n,$$

$q'q'' - qq''' = A'nn'$ ,  $pq''' + qp''' - p'q'' - q'p'' = 2B'nn'$ ,  $p'p'' - pp''' = C'nn'$ , которые мы обозначим через  $\Omega'$ . Величины  $n, n'$  являются здесь квадратными корнями из  $d/D, d'/D$ , причем взятыми с теми же знаками, что и  $n, n'$ ; если поэтому положительный квадратный корень из  $D/D'$  (который является целым числом) положить равным  $k$ , то  $n = kn, n' = kn'$ . Вследствие этого и первых шести равенств из  $\Omega$  и  $\Omega'$  очевидно, что

$$P' = kP, Q' = kQ, R' = kR,$$

$$S' = kS, T' = kT, U' = kU.$$

Поэтому, согласно лемме п. 234, можно определить четыре целых числа  $\alpha, \beta, \gamma, \delta$  с тем свойством, что

$$\alpha p + \beta q = p, \quad \gamma p + \delta q = q,$$

$$\alpha p' + \beta q' = p', \quad \gamma p' + \delta q' = q',$$

и т. д.

и

$$\alpha\delta - \beta\gamma = k.$$

Если подставить эти значения  $p, q, p', q', \dots$  в три последних равенства из  $\Omega'$ , то при помощи равенств  $n = kn, n' = kn'$  и последних трех равенств из  $\Omega$  легко устанавливаются равенства

$$A'\alpha^2 + 2B'\alpha\gamma + C'\gamma^2 = A,$$

$$A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B,$$

$$A'\beta^2 + 2B'\beta\delta + C'\delta^2 = C.$$

Поэтому форма  $F'$  при подстановке  $\alpha, \beta, \gamma, \delta$  (которая является собственной, так как  $\alpha\delta - \beta\gamma = k$  положительно) переходит в  $F$ , т. е. содержит форму  $F$  собственно. Это и требовалось доказать.

Если поэтому форма  $F'$  также составлена из форм  $f, f'$  (таким же образом, как и  $F$ ), то формы  $F, F'$  будут иметь одинаковый определитель и потому будут собственно эквивалентны. Более общо: если форма  $G$  составлена из форм  $g, g'$  таким же образом, как  $F$  соответственно из  $f, f'$  и формы  $g, g'$  собственно эквивалентны формам  $f, f'$ , то и формы  $F, G$  будут собственно эквивалентны.

Так как тот случай, когда обе компонируемые формы входят в композицию прямо, является простейшим, а остальные могут быть легко сведены к нему, мы будем в дальнейшем рассматривать только его, так что если какая-нибудь форма будет названа составленной из двух других, то под этим всегда будет подразумеваться, что она составлена из каждой из них прямо. То же самое ограничение будет иметь место, когда одна форма будет называться преобразуемой в произведение двух других.

## 240

**Теорема.** Если из форм  $f, f'$  составлена форма  $F$ , из  $F, f''$  — форма  $\mathfrak{F}$ , из  $f, f''$  — форма  $F'$ , и из  $F', f'$  — форма  $\mathfrak{F}'$ , то формы  $\mathfrak{F}, \mathfrak{F}'$  собственно эквивалентны.

**Доказательство.** I. Пусть

$$\begin{aligned} f &= ax^2 + 2bxy + cy^2, \\ f' &= a'x'^2 + 2b'x'y' + c'y'^2, \\ f'' &= a''x''^2 + 2b''x''y'' + c''y''^2, \\ F &= AX^2 + 2BXY + CY^2, \\ F' &= A'X'^2 + 2B'X'Y' + C'Y'^2, \\ \mathfrak{F} &= \mathfrak{A}\mathfrak{X}^2 + 2\mathfrak{B}\mathfrak{X}\mathfrak{Q} + \mathfrak{C}\mathfrak{Q}^2, \\ \mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'^2 + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Q}' + \mathfrak{C}'\mathfrak{Q}'^2, \end{aligned}$$

далее, пусть определители этих семи форм равны соответственно  $d, d', d'', D, D', \mathfrak{D}, \mathfrak{D}'$ ; все они имеют одинаковые знаки и относятся один к другому как квадраты. Далее, пусть  $m$  — наибольший общий делитель чисел  $a, 2b, c$ , и аналогичное значение имеют



$m'$ ,  $m''$ ,  $M$  для форм  $f'$ ,  $f''$ ,  $F$ . Тогда, в соответствии с четвертым следствием п. 235,  $D$  есть наибольший общий делитель чисел  $dm'^2$ ,  $d'm^2$  и потому  $Dm''^2$  — наибольший общий делитель чисел  $dm'^2m''^2$ ,  $d'm^2m''^2$ ;  $M = mm'$ ;  $\mathfrak{D}$  — наибольший общий делитель чисел  $Dm''^2$ ,  $p''M^2$  или чисел  $Dm''^2$ ,  $d''m^2m'^2$ . Отсюда следует, что  $\mathfrak{D}$  есть наибольший общий делитель трех чисел  $dm'^2m''^2$ ,  $d'm^2m''^2$ ,  $d''m^2m'^2$ . Но по аналогичной причине и  $\mathfrak{D}'$  есть наибольший общий делитель этих же трех чисел, поэтому, так как  $\mathfrak{D}$  и  $\mathfrak{D}'$  имеют одинаковые знаки, то  $\mathfrak{D} = \mathfrak{D}'$ , т. е. формы  $\mathfrak{F}$ ,  $\mathfrak{F}'$ , имеют одинаковый определитель.

II. Пусть теперь  $F$  переходит в  $ff'$  при подстановке

$$X = pxx' + p'xy' + p''yx' + p'''yy',$$

$$Y = qxx' + q'xy' + q''yx' + q'''yy',$$

и  $\mathfrak{F}$  — в  $Ff''$  при подстановке

$$\mathfrak{X} = pXx'' + p'Xy'' + p''Yx'' + p'''Yy'',$$

$$\mathfrak{Q} = qXx'' + q'Xy'' + q''Yx'' + q'''Yy'',$$

и положительные квадратные корни из  $d/D$ ,  $d'/D$ ,  $D/\mathfrak{D}$ ,  $d''/\mathfrak{D}$  обозначим через  $n$ ,  $n'$ ,  $\mathfrak{N}$ ,  $n''$ . Тогда, согласно п. 235, мы имеем восемнадцать равенств, из которых половина принадлежит преобразованию формы  $F$  в  $ff'$ , и половина — преобразованию формы  $\mathfrak{F}$  в  $Ff''$ . Первое равенство есть  $pq' - qp' = an'$  и по его образцу легко могут быть образованы и остальные которые мы здесь ради краткости должны опустить. Впрочем, величины  $n$ ,  $n'$ ,  $\mathfrak{N}$ ,  $n''$  будут хотя и рациональными, но не обязательно целыми числами.

III. Если значения  $X$ ,  $Y$  подставить в значения  $\mathfrak{X}$ ,  $\mathfrak{Q}$ , то получается следующая подстановка:

$$\begin{aligned} \mathfrak{X} = & (1) xx'x'' + (2) xx'y'' + (3) xy'x'' + (4) xy'y'' + \\ & + (5) yx'x'' + (6) yx'y'' + (7) yy'x'' + (8) yy'y'', \\ \mathfrak{Q} = & (9) xx'x'' + (10) xx'y'' + (11) xy'x'' + (12) xy'y'' + \\ & + (13) yx'x'' + (14) yx'y'' + (15) yy'x'' + (16) yy'y'', \end{aligned}$$

при которой  $\mathfrak{F}$ , очевидно, переходит в произведение  $ff'f''$ . Коэффициент (1) равен  $pp + qp''$ ; значения пятнадцати остальных мы не приводим, так как каждый может определить их без труда. Число

(1) (10) — (2) (9) мы обозначим через (1, 2), число (1) (11) — (3) (9) — через (1, 3), и, вообще,  $(g) (8 + h) — (h) (8 + g)$  — через  $(g, h)$ , где предполагается, что  $g, h$  различные целые числа между 1 и 8, большее из которых есть  $h^*$ . Таким образом, всего получается двадцать восемь знаков. Если обозначить теперь положительные квадратные корни из  $d / \mathfrak{D}$ ,  $d' / \mathfrak{D}$  через  $n$ ,  $n'$  (которые будут равны  $n\mathfrak{A}$ ,  $n'\mathfrak{A}$ ), то мы найдем следующие двадцать восемь равенств:

$$\begin{aligned}
 (1, 2) &= aa'n'', & (3, 5) &= a''b'n - a''bn', \\
 (1, 3) &= aa'n', & (3, 6) &= bb'n'' + b'b''n - bb''n' - \mathfrak{D}nn'n'', \\
 (1, 4) &= ab'n'' + ab''n', & (3, 7) &= a''c'n, \\
 (1, 5) &= a'a''n, & (3, 8) &= bc'n'' + b''c'n, \\
 (1, 6) &= a'b'n'' + a'b''n, & (4, 5) &= b'b''n - bb'n'' - bb''n' + \mathfrak{D}nn'n'', \\
 (1, 7) &= a''bn' + a''b'n, & (4, 6) &= b'c''n - bc''n', \\
 (1, 8) &= bb'n'' + bb''n' + b'b''n + \mathfrak{D}nn'n'', & (4, 7) &= b''c'n - bc'n'', \\
 (2, 3) &= ab''n' - ab'n'', & (4, 8) &= c'c''n, \\
 (2, 4) &= ac''n', & (5, 6) &= ca'n'', \\
 (2, 5) &= a'b''n - a'b'n'', & (5, 7) &= ca''n', \\
 (2, 6) &= a'c''n, & (5, 8) &= b'cn'' + b''cn', \\
 (2, 7) &= ll'n' + b'b''n - bb'n'' - \mathfrak{D}nn'n'', & (6, 7) &= b''cn' - b'cn'', \\
 (2, 8) &= lc''n' + b'c''n, & (6, 8) &= cc''n', \\
 (3, 4) &= ac'n'', & (7, 8) &= cc'n'',
 \end{aligned}$$

которые мы обозначим через  $\Phi$ , и девять других:

$$\begin{aligned}
 (10) (11) - (9) (12) &= an'n''\mathfrak{A}, \\
 (1) (12) - (2) (11) - (3) (10) + (4) (9) &= 2an'n''\mathfrak{B}, \\
 (2) (3) - (1) (4) &= an'n''\mathfrak{C}, \\
 - (9) (16) + (10) (15) + (11) (14) - (12) (13) &= 2bn'n''\mathfrak{A}, \\
 (1) (16) - (2) (15) - (3) (14) + (4) (13) + \\
 + (5) (12) - (6) (11) - (7) (10) + (8) (9) &= 4bn'n''\mathfrak{B}, \\
 - (1) (8) + (2) (7) + (3) (6) - (4) (5) &= 2bn'n''\mathfrak{C}, \\
 (14) (15) - (13) (16) &= cn'n''\mathfrak{A},
 \end{aligned}$$

---

\* Теперешний смысл знака  $(g, h)$  не следует путать с тем, в котором он употреблялся в п. 234; действительно, числа, обозначенные этим знаком, здесь соответствуют тем, на которые в п. 234 умножались числа, обозначенные таким же знаком.

$$(5)(16) - (6)(15) - (7)(14) + (8)(13) = 2cn'n''\mathfrak{B},$$

$$(6)(7) - (5)(8) = cn'n''\mathfrak{C},$$

которые мы обозначим через  $\Psi^*$ .

IV. Давать вывод всех этих 37 равенств было бы слишком долго; достаточно установить лишь некоторые, по образцу которых остальные могут быть доказаны без труда.

1. Мы имеем

$$(1, 2) = (1)(10) - (2)(9) =$$

$$= (pq' - qp')p^2 + (pq''' - qp''' - p'q'' + q'p'')pq +$$

$$+ (p''q''' - q''p''')q^2 = n''(Ap^2 + 2Bpq + Cq^2) = n''aa',$$

а это и есть первое равенство.

2. Имеет место

$$(1, 3) = (1)(11) - (3)(9) = (pq'' - qp'')(pq' - qp') = a''\mathfrak{N}an' = aa''n',$$

а это и есть второе равенство.

3. Имеем

$$(1, 8) = (1)(16) - (8)(9) =$$

$$= (pq' - qp')pp''' + (pq''' - qp''')pq''' - (p'q'' - q'p'')qp''' +$$

$$+ (p''q''' - q''p''')qq''' =$$

$$= n''[App''' + B(pq''' + qp''') + Cqq'''] + b''\mathfrak{N}(pq''' - qp''') =$$

$$= n''(bb' + \sqrt{dd'}) + b''\mathfrak{N}(b'n + bn') = **$$

$$= n''bb' + n'bb'' + nb'b'' + \mathfrak{D}nn'n''.$$

Это восьмое равенство в  $\Phi$ . Установить остальные равенства мы предоставляем читателю.

V. Из равенств  $\Phi$  следующим образом получается, что двадцать восемь чисел  $(1,2), (1,3), \dots$  не имеют общего делителя. Сначала заметим, что двадцать семь произведений по три сомножителя, в которых или первый равен  $n$ , второй равен какому-нибудь из чисел

\* Можно было бы заметить, что мы можем получить 18 других равенств, аналогичных равенствам  $\Psi^*$ , у которых справа вместо сомножителей  $a, 2b, c$  стоят соответственно  $a', 2b', c'$ ;  $a'', 2b'', c''$ ; но эти равенства для нашей цели не нужны, и потому мы их опускаем.

\*\* Это следует из равенства [10] п. 235 и далее. Величина корня  $\sqrt{dd'}$   $\mathfrak{D}nn' = \mathfrak{D}nn'\mathfrak{N}^2 = \mathfrak{D}nn'$ .

$a', 2b' c'$ , третий равен какому-нибудь из чисел  $a'', 2b'', c''$ , или же первый равен  $n'$ , второй — какому-нибудь из чисел  $a, 2b, c$ , третий — какому-нибудь из чисел  $a'', 2b'', c''$ , или, наконец, первый равен  $n''$ , второй — какому-нибудь из чисел  $a, 2b, c$ , третий — какому-нибудь из чисел  $a', 2b', c'$ , — что эти отдельные двадцать семь произведений вследствие равенств  $\Phi$  равны либо каким-нибудь из двадцати восьми чисел  $(1, 2), (1, 3), \dots$ , либо суммам или разностям нескольких из них (например,  $na'a'' = (1, 5)$ ,  $2na'b'' = (1, 6) + (2, 5)$ ,  $4nb'b'' = (1, 8) + (2, 7) + (3, 6) + (4, 5)$ , и подобным же образом для остальных); поэтому, если бы эти числа имели общий делитель, он должен был бы обязательно входить и во все указанные произведения. Но отсюда при помощи п. 40 методом, часто применявшимся ранее, легко получается, что этот же делитель должен входить также и в числа  $dm'm'', n'mm'', n''mm'$ , а потому их квадраты, которые равны  $dm'^2m''^2/\mathfrak{D}$ ,  $d'm^2m''^2/\mathfrak{D}$ ,  $d''m^2m'^2/\mathfrak{D}$ , делятся на его квадрат. Это, однако, невозможно, так как согласно I, наибольший общий делитель трех числителей равен  $\mathfrak{D}$ , и потому сами квадраты не могут иметь никаких общих делителей.

VI. Все это относится к преобразованию формы  $\mathfrak{F}$  в  $ff'f''$  и выводится из преобразований формы  $F$  в  $ff'$  и формы  $\mathfrak{F}$  в  $Ff''$ . Но совершенно аналогичным образом из преобразований формы  $F'$  в  $ff''$  и формы  $\mathfrak{F}'$  в  $F'f'$  выводится следующее преобразование формы  $\mathfrak{F}'$  в  $ff'f''$ :

$$\begin{aligned}\mathfrak{X}' &= (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \dots, \\ \mathfrak{Y}' &= (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \dots\end{aligned}$$

(где все коэффициенты обозначают то же, что и при преобразовании формы  $\mathfrak{F}$  в  $ff'f''$ , и для отличия к каждому из них добавлен штрих), из которого точно так же, как и перед этим, получаются двадцать восемь аналогичных равенствам  $\Phi$  равенств, которые мы обозначим через  $\Phi'$ , и девять других, аналогичных  $\Psi$ , равенств, которые мы обозначим через  $\Psi'$ . Именно, если обозначить  $(1)' (10)'$  —  $(2)' (9)'$  через  $(1, 2)'$ ,  $(1)' (11)'$  —  $(3)' (9)'$  — через  $(1, 3)'$  и т. д., то равенства  $\Phi'$  будут иметь вид

$$(1, 2)' = aa'n'', (1, 3)' = aa''n', \dots,$$

и равенства  $\Psi'$  —

$$(10)'(11)' - (9)'(12)' = a n' n'' \mathfrak{A}', \dots,$$

(Дальнейшее изложение мы представляем ради краткости читателю; впрочем, опытные читатели найдут, что это вычисление не нужно еще раз проводить заново, а можно легко перенести сюда по аналогии первый анализ.) После этого из  $\Phi$  и  $\Phi'$  тотчас же следует

$$(1, 2) = (1, 2)', (1, 3) = (1, 3)', (1, 4) = (1, 4)', (2, 3) = (2, 3)', \dots$$

А отсюда и из того, что  $(1, 2), (1, 3), (2, 3), \dots$  (согласно V) не все имеют общий делитель, получается при помощи леммы п. 234, что можно так определить четыре целых числа  $\alpha, \beta, \gamma, \delta$ , что

$$\begin{aligned} \alpha(1)' + \beta(9)' &= (1), & \alpha(2)' + \beta(10)' &= (2), & \alpha(3)' + \beta(11)' &= (3), \dots, \\ \gamma(1)' + \delta(9)' &= (9), & \gamma(2)' + \delta(10)' &= (10), & \gamma(3)' + \delta(11)' &= (11), \dots \end{aligned}$$

и  $\alpha\delta - \beta\gamma = 1$ .

VII. Отсюда посредством подстановки из первых трех равенств  $\Psi$  значений  $a\mathfrak{A}, a\mathfrak{B}, a\mathfrak{C}$  и из первых трех равенств  $\Psi'$  значений  $a\mathfrak{A}', a\mathfrak{B}', a\mathfrak{C}'$  легко устанавливается, что

$$\begin{aligned} a(\mathfrak{A}\alpha^2 + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma^2) &= a\mathfrak{A}', \\ a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}', \\ a(\mathfrak{A}\beta^2 + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta^2) &= a\mathfrak{C}', \end{aligned}$$

откуда, в случае если  $a$  не равно 0, очевидно, что форма  $\mathfrak{F}$  при собственной подстановке  $\alpha, \beta, \gamma, \delta$  переходит в  $\mathfrak{F}'$ . Если же вместо трех первых равенств из  $\Psi$  и  $\Psi'$  использовать три следующих, то мы найдем три равенства, полностью аналогичных вышеуказанным, в которых лишь вместо сомножителя  $a$  всюду стоит  $b$ , откуда вытекает, что справедливо то же заключение, если только  $b$  не равно 0. Наконец, если использовать последние три равенства из  $\Psi$  и  $\Psi'$ , то мы таким же образом найдем, что наше заключение верно, если только  $c$  не равно 0. Но так как все три числа  $a, b, c$  заведомо не равны нулю одновременно, то форма  $\mathfrak{F}$  обязательно должна переходить при собственной подстановке  $\alpha, \beta, \gamma, \delta$  в  $\mathfrak{F}'$ , и потому она будет этой форме собственно эквивалентна. Это и требовалось доказать.

Такую форму, как  $\mathfrak{F}$  или  $\mathfrak{F}'$ , которая получается, если одну из трех заданных форм скомпонировать с той, которая возникает при композиции двух других, мы будем называть *составленной из этих трех форм*, и из предыдущего пункта вытекает, что *безразлично, в каком порядке компонируются три формы*. Аналогично, если дано любое количество форм  $f, f', f'', f''', \dots$  (определители которых должны относиться один к другому как квадраты), и форма  $f$  компонируется с  $f'$ , получающаяся отсюда форма — с  $f''$ , возникающая после этого форма — с  $f'''$  и т. д., то форма, которая получается в заключение этой операции, называется *составленной из всех форм  $f, f', f'', f''', \dots$* . Легко доказывается, что также и здесь безразлично, в каком порядке формы составляются, т. е. в каком бы порядке эти формы ни составлялись, формы, получающиеся в результате этого составления всегда будут собственно эквивалентны. Далее, ясно, что если формам  $f, f', f'', \dots$  собственно эквивалентны формы  $g, g', g'', \dots$ , то и форма, составленная из последних, будет собственно эквивалентна форме, составленной из первых.

Предыдущие теоремы касаются композиции форм в наиболее общем виде; *теперь мы переходим к специальным применениям*, которыми мы не хотели прерывать последовательность теорем. Сначала мы снова вернемся к задаче п. 236, которую мы ограничим следующими условиями. *Во-первых*, компонируемые формы должны иметь одинаковые определители, т. е.  $d = d'$ ; *во-вторых*,  $m, m'$  должны быть взаимно просты; *в-третьих*, искомая форма должна быть составлена из обеих форм  $f, f'$  прямо. Тогда  $m^2$  и  $m'^2$  также будут взаимно просты и потому наибольший общий делитель чисел  $dm'^2, d'm^2$ , т. е.  $D$ , равен,  $d = d'$  и  $n = n' = 1$ . Четыре величины  $\Omega, \Omega', \Omega'', \Omega'''$ , которые могут быть выбраны по желанию, мы положим соответственно равными — 1, 0, 0, 0, что всегда позволительно, кроме единственного случая, который мы здесь опускаем, когда  $a, a', b + b'$  одновременно равны 0 очевидно, однако, что этот случай может встретиться лишь для форм с положительными

квадратными определителями. Тогда ясно, что  $\mu$  есть наибольший общий делитель чисел  $a, a', b + b'$ , что числа  $\wp', \wp'', \wp'''$  должны быть взяты так, чтобы было

$$\wp' a + \wp'' a' + \wp''' (b + b') = \mu.$$

а  $\wp$  совершенно произвольно. Отсюда, если мы в указанном месте подставим вместо  $p, q, p', q', \dots$  их значения, получаются равенства

$$A = \frac{aa'}{\mu^2}, \quad B = \frac{1}{\mu} [\wp aa' + \wp' ab' + \wp'' a'b + \wp''' (bb' + D)],$$

а  $C$  может быть определено из равенства  $AC = B^2 - D$ , поскольку  $a$  и  $a'$  не равны нулю одновременно.

В этом решении значение  $A$  не зависит, таким образом, от значений  $\wp, \wp', \wp'', \wp'''$  (которые могут быть определены бесконечным числом различных способов); но  $B$  получит другое значение, если придать другие значения этим числам, и есть смысл исследовать, каким образом связаны между собой все значения  $B$ . Для этой цели мы заметим следующее.

I. Как бы ни были определены числа  $\wp, \wp', \wp'', \wp'''$ , получающиеся при этом значения  $B$  все сравнимы между собой по модулю  $A$ . Именно, если предположить, что при

$$\wp = p, \quad \wp' = p', \quad \wp'' = p'', \quad \wp''' = p''' \quad \text{будет} \quad B = \mathfrak{B},$$

а при

$$\wp = p + \mathfrak{d}, \quad \wp' = p' + \mathfrak{d}', \quad \wp'' = p'' + \mathfrak{d}'', \quad \wp''' = p''' + \mathfrak{d}''' \quad \text{будет} \quad B = \mathfrak{B} + \mathfrak{D},$$

то

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''' = 0, \quad aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \mu\mathfrak{D}.$$

Если умножить левую часть второго равенства на  $ap' + a'p'' + (b + b')p'''$ , правую на  $\mu$  и вычесть из первого произведения величину

$$(ab'p' + a'b p'' + (b'^2 + D)p''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}'''),$$

которая вследствие первого равенства, очевидно, равна 0, то после раскрытия скобок и приведения подобных членов мы получим

$$aa'[\mu\mathfrak{d} + ((b' - b)p'' + c'p''')\mathfrak{d}' + ((b - b')p' + cp''')\mathfrak{d}'' - (c'p' + cp'')\mathfrak{d}'''] = \mu^2\mathfrak{D},$$

откуда следует, что  $\mu^2\mathfrak{D}$  делится на  $aa'$ , или  $\mathfrak{D}$  делится на  $aa'/\mu^2$ , т. е. на  $A$ , и

$$\mathfrak{B} \equiv (\mathfrak{B} + \mathfrak{D}) \pmod{A}.$$

II. Если для значений  $p, p', p'', p'''$  чисел  $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$  будет  $B = \mathfrak{B}$ , то можно найти другие значения этих чисел, для которых  $B$  принимает любое заданное сравнимое с  $\mathfrak{B}$  по модулю  $A$  значение, скажем,  $\mathfrak{B} + kA$ . Сначала заметим, что четыре числа  $\mu, c, c', b - b'$  не могут иметь общих делителей; действительно, если бы они имели общий делитель, то он входил бы в шесть чисел  $a, a', b + b', c, c', b - b'$ , а потому также как в  $a, 2b, c$ , так и в  $a', 2b', c'$ , а, следовательно, в  $m, m'$ , которые, однако, по предположению взаимно просты. Поэтому могут быть указаны четыре целых числа  $h, h', h'', h'''$  с тем свойством, что

$$h\mu + h'c + h''c' + h'''(b - b') = 1.$$

Если сделать это и положить

$$kh = \mathfrak{d}, \quad k[h''(b + b') - h'''a'] = \mu\mathfrak{d}',$$

$$k[h'(b + b') + h'''a] = \mu\mathfrak{d}'', \quad -k(h'a' + h''a) = \mu\mathfrak{d}''',$$

то числа  $\mathfrak{d}, \mathfrak{d}', \mathfrak{d}'', \mathfrak{d}'''$ , очевидно, будут целыми; далее, легко устанавливается, что

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''' = 0,$$

$$\begin{aligned} aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' &= \\ &= \frac{aa'k}{\mu} [\mu h + ch' + c'h'' + (b - b')h'''] = \mu kA. \end{aligned}$$

Из первого равенства вытекает, что и  $p' + \mathfrak{d}, p' + \mathfrak{d}', p'' + \mathfrak{d}'', p''' + \mathfrak{d}'''$  могут быть взяты в качестве  $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ , а из второго, что эти значения дают  $B = \mathfrak{B} + kA$ .

Отсюда видно, что  $B$  всегда может быть определено так, что оно будет лежать между 0 и  $A - 1$  включительно, если  $A$  положительно, и между 0 и  $-A - 1$ , если  $A$  отрицательно.



Из равенств

$$\wp'a + \wp''a' + \wp'''(b + b') = \mu, \quad B = \frac{1}{\mu} [\wp'aa' + \wp'ab' + \wp''a'b + \wp'''(bb' + D)]$$

следует

$$B = b + \frac{a}{\mu} [\wp'a' + \wp'(b' - b) - \wp'''c] = b' + \frac{a'}{\mu} [\wp'a + \wp''(b - b') - \wp'''c'],$$

и потому

$$B \equiv b \pmod{\frac{a}{\mu}}, \quad B \equiv b' \pmod{\frac{a'}{\mu}}.$$

Если  $a/\mu$ ,  $a'/\mu$  взаимно просты, то между 0 и  $A - 1$  (или между 0 и  $-A - 1$  когда  $A$  отрицательно) будет лежать только одно единственное число, которое  $\equiv b \pmod{a/\mu}$  и  $\equiv b' \pmod{a'/\mu}$ ; если его положить равным  $B$  и  $\frac{B^2 - D}{A} = C$ , то форма  $(A, B, C)$  будет, очевидно, составлена из форм  $(a, b, c)$ ,  $(a', b', c')$ . Таким образом, в этом случае для отыскания скомпонированной формы не нужно больше беспокоиться о числах  $\wp$ ,  $\wp'$ ,  $\wp''$ ,  $\wp'''$  \*.

Например, если отыскивается форма, составленная из форм  $(10, 3, 11)$ ,  $(15, 2, 7)$ , то  $a, a', b + b'$  равны соответственно 10, 15, 5;  $\mu = 5$ ; отсюда  $A = 6$ ;  $B \equiv 3 \pmod{2}$  и  $\equiv 2 \pmod{3}$ , тем самым  $B = 5$ , и искомая форма есть  $(6, 5, 21)$ . Впрочем, условие, что  $a/\mu$ ,  $a'/\mu$  взаимно просты, вполне эквивалентно условию, что оба числа  $a, a'$  не должны иметь большего общего делителя, чем три числа  $a, a', b + b'$ , или, что сводится к тому же, что наибольший общий делитель чисел  $a, a'$  должен входить также и в число  $b + b'$ . Можно, в частности, указать следующие специальные случаи.

1. Если даны две формы  $(a, b, c)$ ,  $(a', b', c')$  с одним и тем же определителем  $D$  и тем свойством, что наибольший общий делитель чисел  $a, 2b, c$  взаимно прост с наибольшим общим делителем чисел  $a', 2b', c'$  и, далее,  $a$  взаимно просто с  $a'$ , то мы найдем состав-

---

\* Что всегда достигается при помощи сравнений

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b + b')B}{\mu} \equiv \frac{bb' + D}{\mu} \pmod{A}.$$

ленную из них форму  $(A, B, C)$ , если положим  $A = aa'$ ,  $B \equiv b \pmod{a}$  и  $\equiv b' \pmod{a'}$ ,  $C = \frac{B^2 - D}{A}$ . Этот случай всегда имеет место, когда одна из компонируемых форм является главной формой, т. е. когда  $a = 1$ ,  $b = 0$ ,  $c = -D$ . Тогда  $A = a'$ ,  $B$  можно положить равным  $b'$ , откуда следует, что  $C = c'$ . Таким образом, форма, составленная из главной формы и какой-нибудь второй формы с тем же определителем, есть сама эта вторая форма.

2. Если компонируются две противоположные собственно примитивные формы, например,  $(a, b, c)$  и  $(a, -b, c)$ , то  $\mu = a$ . Из этого легко видно, что главная форма  $(1, 0, -D)$  будет составленной из них.

3. Если дано сколько угодно собственно примитивных форм  $(a, b, c)$ ,  $(a', b', c')$ ,  $(a'', b'', c'')$ , ... с одним и тем же определителем  $D$ , первые члены которых  $a, a', a'', \dots$  являются попарно взаимно простыми числами, то мы найдем составленную из них форму  $(A, B, C)$ , если положим  $A$  равным произведению всех чисел  $a, a', a'', \dots$ ,  $B$  — сравнимым с отдельными  $b, b', b'', \dots$  соответственно по модулям  $a, a', a'', \dots$ , и  $C = \frac{B^2 - D}{A}$ . Действительно, легко видеть, что формой, составленной из двух форм  $(a, b, c)$ ,  $(a', b', c')$ , будет  $(aa', B, (B^2 - D)/aa')$ , формой, составленной из нее и из  $(a'', b'', c'')$  будет  $(aa'a'', B, (B^2 - D)/aa'a'')$  и т. д.

4. Обратно, если дана собственно примитивная форма  $(A, B, C)$  с определителем  $D$ , и член  $A$  разложен на любое число попарно взаимно простых сомножителей  $a, a', a'', \dots$ , далее, числа  $b, b', b'', \dots$  или равны  $B$ , или по крайней мере сравнимы с  $B$  соответственно по модулям  $a, a', a'', \dots$ , и положено  $ac = b^2 - D$ ,  $a'c' = b'^2 - D$ ,  $a''c'' = b''^2 - D$ , то форма  $(A, B, C)$  будет составлена из форм  $(a, b, c)$ ,  $(a', b', c')$ ,  $(a'', b'', c'')$ , ..., или будет разложима на эти формы. Без труда доказывается, что такая же теорема имеет место и тогда, когда форма  $(A, B, C)$  является несобственно примитивной или произведенной. Этим способом, следовательно, каждая форма может быть разложена на другие формы с тем же определителем, первые члены которых все являются или простыми числами, или степенями простых чисел. Такое разложение часто может быть с пользой применено, когда из нескольких заданных форм нужно скомпонировать одну. Например, если отыскивается форма, составленная из форм

(3, 1, 134), (10, 3, 41), (15, 2, 27), то разлагаем вторую форму на следующие: (2, 1, 201), (5, —2, 81), — третью — на (3, —1, 134), (5, 2, 81); тогда форма, составленная из пяти форм (3, 1, 134), (2, 1, 201), (5, —2, 81), (3, —1, 134), (5, 2, 81), в каком бы порядке они ни брались, будет, очевидно, составлена также из трех заданных форм. Но при композиции первой и четвертой форм получается главная форма (1, 0, 401); она же возникает при композиции третьей и пятой форм; поэтому при композиции всех пяти форм получается форма (2, 1, 201).

5. Вследствие большой пользы этого метода стоит потрудиться над тем, чтобы развить его еще несколько далее. Из предыдущего замечания вытекает, что проблема композиции любого числа заданных собственно примитивных форм с одинаковым определителем может быть сведена к композиции форм, первые члены которых являются степенями простых чисел (ибо простое число может рассматриваться как первая степень самого себя). Поэтому мы хотим специально рассмотреть случай, когда компонируются две собственно примитивные формы  $(a, b, c)$ ,  $(a', b', c')$ , у которых  $a$  и  $a'$  являются степенями одного и того же простого числа. Если, таким образом,  $a = h^x$ ,  $a' = h^\lambda$ , где  $h$  обозначает простое число, и если мы предположим (что допустимо), что  $x$  не меньше чем  $\lambda$ , то  $h^\lambda$  будет наибольшим общим делителем чисел  $a$ ,  $a'$ , и если он, кроме того, входит в  $b + b'$ , то мы имеем случай, рассмотренный в начале этого пункта и  $(A, B, C)$  будет составлена из заданных форм, если положить  $A = h^{x-\lambda}$ ,  $B \equiv b \pmod{h^{x-\lambda}}$  и  $\equiv b' \pmod{1}$  (это последнее условие можно, конечно, отбросить), и  $C = \frac{B^2 - D}{A}$ . Если же  $h^\lambda$  не входит в  $b + b'$ , то наибольший общий делитель этих чисел обязательно сам будет степенью  $h$ ; если он равен  $h^\nu$ , то  $\nu < \lambda$  (если случайно  $h^\lambda$  и  $b + b'$  взаимно просты, нужно положить  $\nu = 0$ ). Если поэтому  $\mathfrak{P}'$ ,  $\mathfrak{P}''$ ,  $\mathfrak{P}'''$  определены так, что

$$\mathfrak{P}' h^x + \mathfrak{P}'' h^\lambda + \mathfrak{P}''' (b + b') = h^\nu,$$

а  $\mathfrak{P}$  взято произвольно, то форма  $(A, B, C)$  будет составлена из заданных форм, если положить

$$A = h^{x+\lambda-2\nu}, \quad B = b + h^{x-\nu} [\mathfrak{P} h^\lambda - \mathfrak{P}' (b' - b) - \mathfrak{P}''' c], \quad C = \frac{B^2 - D}{A}.$$

Но легко видеть, что в этом случае и  $\mathfrak{P}'$  можно брать произвольно, так что если положить  $\mathfrak{P} = \mathfrak{P}' = 0$ , то получается

$$B = b - \mathfrak{P}''' ch^{\kappa-\nu},$$

или вообще

$$B = kA + b - \mathfrak{P}''' ch^{\kappa-\nu},$$

где  $k$  обозначает любое число (предыдущий пункт). В эту очень простую формулу входит только  $\mathfrak{P}'''$ , которое есть значение выражения  $\frac{h^\nu}{b+b'} \pmod{h^\lambda}$  \*. Например, если отыскивается форма, составленная из форм (16, 3, 19) и (8, 1, 37), то  $h = 2$ ,  $\kappa = 4$ ,  $\lambda = 3$ ,  $\nu = 2$ . Поэтому  $A = 8$ ,  $\mathfrak{P}'''$  — значение выражения  $\frac{4}{4} \pmod{8}$ ; одним из них является 1, поэтому  $B = 8k - 73$ , и тем самым, если положить  $k = 9$ , то  $B = -1$  и  $C = 37$ . Следовательно, (8, -1, 37) является искомой формой.

Если, таким образом, дано любое число форм, первые члены которых все являются степенями простых чисел, то нужно посмотреть, будут ли первые члены некоторых из них степенями одного и того же простого числа, и их скомпонировать между собой по только что указанному правилу. Тогда получатся формы, первые члены которых все еще являются степенями простых чисел, но уже сплошь различных; поэтому форма, составленная из них, может быть определена в соответствии с третьим замечанием. Если, например, даны формы (3, 1, 17), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11), то из первой и пятой получается форма (27, 7, 7), из второй и четвертой — форма (16, -6, 11), из нее и из шестой — форма (1, 0, 140), которая может быть отброшена. Поэтому остаются только формы (5, 0, 28) и (27, 7, 7), из которых получается форма (135, -20, 4), вместо которой может быть взята также собственно

---

\* Или выражения  $\frac{1}{b+b'} \pmod{h^{\lambda-\nu}}$ , откуда следует, что

$$B \equiv b - \frac{ch^{\kappa-\nu}}{\frac{b+b'}{h^\nu}} \equiv \frac{(D+bb') : h^\nu}{(b+b') : h^\nu} \pmod{A}.$$

эквивалентная ей форма  $(4, 0, 35)$ . Таким образом, она получается в результате композиции шести заданных форм.

Впрочем, из этого же источника может быть почерпнуто еще много других полезных для применения специальных приемов; но чтобы не быть слишком пространными, мы опускаем более подробный разбор этого предмета и обращаемся к другим, более трудным вопросам.

## 244

Если число  $a$  может быть представлено какой-нибудь формой  $f$ , а число  $a'$  — формой  $f'$ , и форма  $F$  преобразуема в  $ff'$ , то без труда видно, что произведение  $aa'$  представимо формой  $F$ . Отсюда тотчас же следует, что если определители этих форм отрицательны, форма  $F$  положительна, если формы  $f, f'$  либо обе положительны, либо обе отрицательны, и наоборот, форма  $F$  отрицательна, если одна из форм  $f, f'$  положительна, а другая отрицательна. Мы хотим специально остановиться на случае, который мы рассматривали в предыдущем пункте, именно, когда  $F$  составлена из  $f, f'$ , и  $f, f'$ ,  $F$  имеют один и тот же определитель  $D$ . Если мы, кроме того, предположим, что представления чисел  $a, a'$  формами  $f, f'$  осуществляются при взаимно простых значениях неизвестных, и что первое представление принадлежит значению  $b$  выражения  $\sqrt{D} \pmod{a}$ , а второе — значению  $b'$  выражения  $\sqrt{D} \pmod{a'}$ , и положим  $b^2 - D = ac$ ,  $b'^2 - D = a'c'$ , то, согласно п. 168, формы  $(a, b, c), (a', b', c')$  будут собственно эквивалентны формам  $f, f'$ , вследствие чего  $F$  составлена также и из двух первых. Но из этих же форм составлена форма  $(A, B, C)$ , если мы, обозначив наибольший общий делитель чисел  $a, a', b + b'$  через  $\mu$ , положим  $A = \frac{aa'}{\mu^2}$ ,  $B \equiv b$  и  $\equiv b'$  соответственно по модулям  $a/\mu, a'/\mu$ , и  $AC = B^2 - D$ . Следовательно, эта форма будет собственно эквивалентна форме  $F$ . Но число  $aa'$  представляется формой  $Ax^2 + 2Bxy + Cy^2$ , если положить  $x = \mu, y = 0$ ; эти значения имеют общий делитель  $\mu$ ; поэтому  $aa'$  может быть представлено и формой  $F$  так, что значения неизвестных имеют наибольший общий делитель  $\mu$  (п. 166). Поэтому если  $\mu = 1$ , то число  $aa'$  может быть представлено формой  $F$  при взаим-

но простых значениях неизвестных, и это представление будет принадлежать значению выражения  $\sqrt{D} \pmod{aa'}$ , равному  $B$ , которое по модулям  $a, a'$  сравнимо соответственно с числами  $b, b'$ . Условие  $\mu = 1$  заведомо выполняется, если  $a, a'$  взаимно просты; вообще же оно выполняется всегда, когда наибольший общий делитель  $a, a'$  взаимно прост с  $b + b'$ .

## Композиция порядков

245

**Теорема.** Если форма  $f$  принадлежит тому же порядку, что и  $g$ , и точно так же  $f'$  из того же порядка, что и  $g'$ , то форма  $F$ , составленная из  $f, f'$ , будет иметь тот же определитель и принадлежать тому же порядку, что и составленная из  $g, g'$  форма  $G$ .

**Доказательство.** Пусть формы  $f, f', F$  соответственно равны  $(a, b, c), (a', b', c'), (A, B, C)$ , а их определители  $d, d', D$ . Далее, пусть наибольший общий делитель чисел  $a, 2b, c$  равен  $m$ , а наибольший общий делитель чисел  $a, b, c$  равен  $\mathfrak{m}$ , и аналогичные значения имеют  $m', \mathfrak{m}'$  по отношению к форме  $f'$  и  $M, \mathfrak{M}$  по отношению к форме  $F$ . Тогда порядок формы  $f$  определяется числами  $d, m, \mathfrak{m}$ , вследствие чего те же числа будут принадлежать и форме  $g$ ; по той же причине числа  $d', m', \mathfrak{m}'$  будут для формы  $g'$  тем же, что и для формы  $f'$ . Но в соответствии с п. 235 числа  $D, M, \mathfrak{M}$  определяются числами  $d, d', m, m', \mathfrak{m}, \mathfrak{m}'$ ; именно,  $D$  есть наибольший общий делитель  $dm'^2$  и  $d'm^2$ , далее,  $M = mm'$  и  $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$  (если одновременно  $m = \mathfrak{m}$  и  $m' = \mathfrak{m}'$ ) или  $= 2\mathfrak{m}\mathfrak{m}'$  (если  $m = 2\mathfrak{m}$  или  $m' = 2\mathfrak{m}'$ ). Так как эти свойства чисел  $D, M, \mathfrak{M}$  получаются из того, что  $F$  составлено из  $f, f'$ , то очевидно, что  $D, M, \mathfrak{M}$  должны иметь те же значения и для  $G$ , и потому  $G$  будет из того же порядка, что и  $F$ . Это и требовалось доказать.

На основании этого мы будем называть порядок, в котором содержится  $F$ , составленным из порядков, в которых содержатся  $f, f'$ . Так, например, из двух собственно примитивных порядков всегда составляется порядок такого же типа, а из собственно примитивного и несобственно примитивного — несобственно примитивный.

Аналогичным образом следует понимать и такие выражения, когда порядок называется составленным из нескольких других порядков.

## Композиция родов

246

**Задача.** Пусть даны две любые примитивные формы  $f, f'$ , при композиции которых получается форма  $F$ ; тогда, зная роды, которым принадлежат  $f, f'$ , нужно определить род, к которому относится  $F$ .

**Решение.** I. Рассмотрим сначала случай, когда по крайней мере одна из форм  $f, f'$ , например, первая, собственно примитивна, и обозначим определители форм  $f, f', F$  соответственно через  $d, d', D$ . Тогда  $D$  есть наибольший общий делитель чисел  $dm'^2, d'$ , где  $m'$  равно 1 или 2 в зависимости от того, собственно или несобственно примитивна форма  $f'$ . В первом случае  $F$  будет принадлежать собственно примитивному порядку, во втором — несобственно примитивному порядку. Род же формы  $F$  определяется ее специальными характеристиками как по отношению к отдельным нечетным простым делителям числа  $D$ , так, в некоторых случаях, и по отношению к числам 4 и 8. Мы должны поэтому определить их отдельно.

1. Если  $p$  какой-нибудь нечетный простой делитель  $D$ , то он обязательно входит также в  $d, d'$ , и потому среди характеров форм  $f, f'$  обязательно будут фигурировать также и их отношения к  $p$ . Если теперь число  $a$  представляется формой  $f$ , а число  $a'$  — формой  $f'$ , то произведение  $aa'$  будет представимо формой  $F$ . Поэтому, если как формой  $f$ , так и формой  $f'$  представляются квадратичные вычеты по модулю  $p$  (не делящиеся на  $p$ ), то и формой  $F$  могут представляться квадратичные вычеты по модулю  $p$ , т. е. если каждая из форм  $f, f'$  имеет характер  $Rp$ , то и форма  $F$  будет иметь этот же характер. По той же причине  $F$  будет иметь характер  $Rp$ , если каждая из форм  $f, f'$  имеет характер  $Np$ ; наоборот,  $F$  имеет характер  $Np$ , если одна из форм  $f, f'$  имеет характер  $Rp$ , а другая — характер  $Np$ .

2. Если в полный характер формы  $F$  входит отношение к числу 4, то такое отношение должно фигурировать и в характерах

форм  $f, f'$ . Действительно, это имеет место только тогда, когда  $D \equiv 0$  или  $\equiv 3 \pmod{4}$ . Если  $D$  делится на 4, то также и  $dm'^2$  и  $d'$  делятся на 4, откуда тотчас же вытекает, что форма  $f'$  не может быть несобственно примитивной и потому  $m' = 1$ . Поэтому как  $d$ , так и  $d'$  делятся на 4, и в характерах обеих форм фигурирует отношение к числу 4. Если  $D \equiv 3 \pmod{4}$ , то  $D$  входит в  $d, d'$ ; отношения являются квадратами, и потому  $d, d'$  также обязательно или  $\equiv 0$ , или  $\equiv 3 \pmod{4}$ , и среди характеров форм  $f, f'$  находятся их отношения к числу 4. Отсюда тем же способом, как и в (1), следует, что характер формы  $F$  есть 1, 4, если обе формы  $f, f'$  имеют или характер 1, 4, или характер 3, 4, и, наоборот, характер формы  $F$  есть 3, 4, если одна из форм  $f, f'$  имеет характер 1, 4, а другая — характер 3, 4.

3. Если  $D$  делится на 8, то делится на 8 также и  $d'$ ; поэтому форма  $f'$  заведомо собственно примитивна,  $m' = 1$  и  $d$  тоже делится на 8. Поэтому среди характеров формы  $F$  какой-нибудь из характеров 1, 8; 3, 8; 5, 8; 7, 8 может встретиться только тогда, когда как в характере формы  $f$ , так и в характере формы  $f'$  фигурирует подобное отношение к числу 8. Но тем же способом, как и раньше, легко устанавливается, что характер формы  $F$  есть 1, 8, если  $f$  и  $f'$  имеют по отношению к числу 8 одинаковый характер; что характер формы  $F$  есть 3, 8, если одна из форм  $f, f'$  имеет характер 1, 8, а другая — характер 3, 8, или если одна имеет характер 5, 8, а другая — характер 7, 8; что форма  $F$  обладает характером 5, 8, если формы  $f, f'$  имеют характеры 1, 8 и 5, 8 или характеры 3, 8 и 7, 8; наконец,  $F$  имеет характер 7, 8, если  $f, f'$  имеют характеры 1, 8 и 7, 8 или 3, 8 и 5, 8.

4. Если  $D \equiv 2 \pmod{8}$ , то  $d'$  или  $\equiv 0$ , или  $\equiv 2 \pmod{8}$ ; поэтому  $m' = 1$ , и потому также и  $d$  или  $\equiv 0$ , или  $\equiv 2 \pmod{8}$ . Однако оба числа  $d$  и  $d'$  не могут делиться на 8, так как  $D$  является их наибольшим общим делителем. Поэтому форме  $F$  может быть придан тот или иной из двух характеров 1 и 7, 8; 3 и 5, 8 только тогда, когда или обе формы  $f, f'$  обладают одним из этих характеров, или одна из них имеет один из этих характеров, а другая один из следующих характеров: 1, 8; 3, 8; 5, 8; 7, 8. Отсюда легко получается, что характер формы  $F$  может быть определен по следующей



таблице, где находящийся слева характер относится к одной из форм  $f, f'$ , а находящийся вверху — к другой:

|          |                                  |                                  |
|----------|----------------------------------|----------------------------------|
|          | 1 и 7, 8<br>или 1, 8<br>или 7, 8 | 3 и 5, 8<br>или 3, 8<br>или 5, 8 |
| 1 и 7, 8 | 1 и 7, 8                         | 3 и 5, 8                         |
| 3 и 5, 8 | 3 и 5, 8                         | 1 и 7, 8                         |

5. Подобным же образом доказывается, что форме  $F$  не может быть придан тот или иной из двух характеров 1 и 3, 8; 5 и 7, 8, если только одним из них не обладает по крайней мере одна из форм  $f, f'$ , в то время как другая имеет или тоже один из этих характеров, или один из следующих: 1, 8; 3, 8; 5, 8; 7, 8, причем характер формы  $F$  может быть найден при помощи следующей таблицы, в которой характеры форм  $f, f'$  находятся слева и вверху:

|          |                                  |                                  |
|----------|----------------------------------|----------------------------------|
|          | 1 и 3, 8<br>или 1, 8<br>или 3, 8 | 5 и 7, 8<br>или 5, 8<br>или 7, 8 |
| 1 и 3, 8 | 1, 3, 8                          | 5 и 7, 8                         |
| 5 и 7, 8 | 5 и 7, 8                         | 1 и 3, 8                         |

II. Если обе формы  $f, f'$  несобственно примитивны, то  $D$  есть наибольший общий делитель чисел  $4d, 4d'$ , или  $D/4$  — наибольший общий делитель чисел  $d, d'$ . Отсюда легко следует, что и  $d$ , и  $d'$ , и  $\frac{1}{4} D \equiv 1 \pmod{4}$ . Если положить  $F = (A, B, C)$ , то наибольший общий делитель чисел  $A, B, C$  равен 2, и наибольший общий

делитель чисел  $A$ ,  $2B$ ,  $C$  равен 4. Поэтому  $F$  есть форма, произведенная из несобственно примитивной формы  $(A/2, B/2, C/2)$ ; определитель последней равен  $D/4$ , и ее род будет определять род формы  $F$ . Но характер первой формы, так как она несобственно примитивна, не содержит отношений к 4 или 8, а лишь отношения к отдельным нечетным простым делителям числа  $D/4$ . Но так как, очевидно, все эти делители входят в  $d$ ,  $d'$ , и половина каждого произведения двух сомножителей, один из которых представляется формой  $f$ , а другой формой  $f'$ , может быть представлена формой  $\left(\frac{A}{2}, \frac{B}{2}, \frac{C}{2}\right)$ , то легко видеть, что характер этой формы по отношению к каждому входящему в  $D/4$  нечетному простому числу есть  $Rp$ , как тогда, когда  $2Rp$  и формы  $f$ ,  $f'$  имеют по отношению к  $p$  один и тот же характер, так и тогда, когда  $2Np$  и характеры форм  $f$ ,  $f'$  по отношению к  $p$  противоположны, и что, напротив, характер формы  $\left(\frac{A}{2}, \frac{B}{2}, \frac{C}{2}\right)$  есть  $Np$ , как тогда, когда  $f$ ,  $f'$  имеют одинаковые характеры по отношению к  $p$ , и  $2Np$ , так и тогда, когда  $f$ ,  $f'$  имеют противоположные характеры, и  $2Rp$ .

## 247

Из решения предыдущей проблемы вытекает, что если  $g$  — примитивная форма из того же порядка и того же рода, что и  $f$ , и точно так же  $g'$  — примитивная форма из того же порядка и того же рода, что и  $f'$ , то форма, составленная из  $g$  и  $g'$ , принадлежит тому же роду, что и форма, составленная из  $f$ ,  $f'$ . Отсюда непосредственно получается понятие **рода, составленного из двух** (или нескольких) *других родов*. Далее, из этого же следует, что если  $f$ ,  $f'$  имеют одинаковый определитель, и  $f$  — форма из главного рода, а  $F$  составлена из  $f$ ,  $f'$ , то  $F$  будет из того же рода, что и  $f'$ ; поэтому главный род при композиции с другими родами всегда может быть отброшен. Если же при сохранении остальных условий  $f$  не из главного рода, а  $f'$  — примитивная форма, то  $F$  заведомо будет не из того рода, что  $f'$ . Если, наконец,  $f$ ,  $f'$  — собственно примитивные формы одного и того же рода, то  $F$  будет из главного рода; если же  $f$ ,  $f'$  обе несобственно примитивные формы с

одинаковым определителем, но из различных родов, то  $F$  не может принадлежать главному роду. Поэтому если какая-нибудь собственно примитивная форма *компонируется сама с собой*, то получающаяся при этом форма, которая тоже собственно примитивна и имеет этот же определитель, обязательно будет принадлежать главному роду.

## 248

**Задача.** Пусть даны две любые формы  $f, f'$ , из которых составлена форма  $F$ ; нужно по родам форм  $f, f'$  определить, к какому роду принадлежит форма  $F$ .

**Решение.** Пусть  $f = (a, b, c)$ ,  $f' = (a', b', c')$ ,  $F = (A, B, C)$ , далее,  $m$  — наибольший общий делитель чисел  $a, b, c$ , и  $m'$  — наибольший общий делитель чисел  $a', b', c'$ , так что формы  $f, f'$  произведены из примитивных форм  $(a/m, b/m, c/m)$ ,  $(a'/m', b'/m', c'/m')$ , которые мы соответственно обозначим через  $\mathfrak{f}, \mathfrak{f}'$ . Если теперь по крайней мере одна из форм  $\mathfrak{f}, \mathfrak{f}'$  собственно примитивна, то наибольший общий делитель чисел  $A, B, C$  будет равен  $mm'$ , и потому  $F$  будет произведена из примитивной формы  $(A/mm', B/mm', C/mm') = \mathfrak{F}$ , откуда следует, что род формы  $F$  зависит от рода формы  $\mathfrak{F}$ . Но легко убедиться, что  $\mathfrak{F}$  переходит в  $\mathfrak{f}\mathfrak{f}'$  при той же подстановке, при которой  $F$  переходит в  $ff'$  и что тем самым форма  $\mathfrak{F}$  составлена из форм  $\mathfrak{f}\mathfrak{f}'$ , и ее род может быть определен в соответствии с задачей п. 246. Если же обе формы  $\mathfrak{f}, \mathfrak{f}'$  не собственно примитивны, то наибольший общий делитель чисел  $A, B, C$  равен  $2mm'$ , и форма  $\mathfrak{F}$  также и в этом случае составлена из форм  $\mathfrak{f}, \mathfrak{f}'$ , и, очевидно, произведена из собственно примитивной формы  $(A/2mm', B/2mm', C/2mm')$ . Род этой формы может быть поэтому определен по п. 246, а так как  $F$  произведена из этой формы, то тем самым тотчас же становится известным и род формы  $F$ .

Из этого решения вытекает, что изложенная в предыдущем пункте теорема для примитивных форм, именно, что *если формы  $f', g'$  из одних и тех же родов, что и формы  $f, g$ , то форма, составленная из  $f' g'$ , принадлежит тому же роду, что и форма, составленная из  $f, g$ , сохраняет силу для любых форм.*

## Композиция классов

249

**Теорема.** *Если формы  $f, f'$  из тех же порядков, родов и классов, что и соответственно формы  $g, g'$ , то и форма, составленная из  $f, f'$ , будет из того же класса, что и форма, составленная из  $g$  и  $g'$ .*

Из этой теоремы, справедливость которой немедленно следует из п. 239, делается непосредственно ясным понятие класса, составленного из двух или из нескольких заданных классов.

Если некоторый класс  $K$  компонируется с главным классом, то получается снова класс  $K$ , т. е. главный класс при композиции с другими классами того же определителя может отбрасываться. При композиции двух противоположных классов всегда получается главный класс того же определителя (ср. п. 243). Так как каждый двусторонний класс противоположен самому себе, то при композиции каждого собственно примитивного двустороннего класса с самим собой получается главный класс того же определителя.

Верно и обращение последней теоремы, именно: *если при композиции собственно примитивного класса  $K$  с самим собой получается главный класс  $H$  того же определителя, то  $K$  обязательно двусторонний класс.* Действительно, если  $K'$  есть класс, противоположный классу  $K$ , то из трех классов  $K, K, K'$  при композиции получается тот же класс, что и из  $H$  и  $K'$ ; но из первых получается  $K$  (так как  $K$  и  $K'$  дают главный класс  $H$ , а он и  $K$  снова дают  $K$ ), а из вторых —  $K'$ . Тем самым  $K$  совпадает с  $K'$  и потому является двусторонним классом.

Далее, может быть выведена следующая теорема: *если классы  $K, L$  соответственно противоположны классам  $K', L'$ , то и класс, составленный из  $K$  и  $L$ , будет противоположен классу, составленному из  $K'$  и  $L'$ .* Пусть формы  $f, g, f', g'$  принадлежат соответственно классам  $K, L, K', L'$ ; пусть форма  $F$  составлена из  $f$  и  $g$ , а форма  $F'$  — из  $f'$  и  $g'$ . Так как формы  $f'$  и  $f$ , так же, как и формы  $g'$  и  $g$ , несобственно эквивалентны, а  $F$  составлена из каждой из двух форм  $f, g$  прямо, то  $F$  будет составлена и из форм  $f', g'$ , но из каждой обратно. Поэтому каждая форма, которая несобственно эквива-

лентна форме  $F$ , прямо составлена из  $f'$  и  $g'$ , и потому собственно эквивалентна форме  $F'$  (пп. 238, 239), вследствие чего  $F$ ,  $F'$  несобственно эквивалентны, и классы, которым они принадлежат, противоположны.

Отсюда следует, что если компонируется двусторонний класс  $K$  с двусторонним классом  $L$ , то всегда получается двусторонний класс. Действительно, это есть класс, который составлен из классов, противоположных классам  $K$ ,  $L$ , и потому он противоположен сам себе, ибо эти классы противоположны сами себе.

Наконец, заметим, что если даны два любых класса  $K$ ,  $L$  с одинаковым определителем, из которых первый собственно примитивен, то всегда можно найти класс  $M$  с тем же определителем, который, будучи скомпонирован с  $K$ , дает  $L$ . Очевидно, мы добьемся этого, если возьмем за  $M$  класс, который составлен из  $L$  и класса, противоположного классу  $K$ ; одновременно очень легко усмотреть, что этот класс является единственным, обладающим таким свойством, или что различные классы одного и того же определителя, будучи скомпонированы с одним и тем же собственно примитивным классом, дают различные классы.

Композицию классов удобно обозначать знаком сложения  $+$ , и, точно так же, тождественность классов — знаком равенства. Тогда только что высказанная теорема может быть выражена следующим образом. Если  $K'$  есть класс, противоположный классу  $K$ , то  $K + K'$  есть главный класс того же определителя, и тем самым  $K + K' + L = L$ ; если поэтому положить  $K' + L = M$ , то  $K + M = L$ , что и требовалось. Если же, кроме  $M$ , имелся бы еще и другой класс  $M'$ , который обладал бы тем же свойством, т. е. если бы было  $K + M' = L$ , то имело бы место  $K + K' + M' = L + K' = M$ , откуда следует, что  $M' = M$ . Если составляются несколько одинаковых классов, то это можно (по образцу умножения) обозначать, ставя впереди число, указывающее их количество, так что, например,  $2K$  означает то же, что  $K + K$ ,  $3K$  — то же, что  $K + K + K$ , и т. д. Те же обозначения можно было бы перенести и на формы, так что  $(a, b, c) + (a', b', c')$  означало бы форму, составленную из форм  $(a, b, c)$ ,  $(a', b', c')$ ; но чтобы избежать всякой двусмысленности, мы предпочитаем отказаться от этого сокращения,

тем более, что знаку  $\sqrt{M(a, b, c)}$  мы уже придали специальное значение. Мы будем говорить, что класс  $2K$  получается удвоением класса  $K$ , класс  $3K$  — утроением класса  $K$ , и т. д.

250

Если  $D$  есть число, делящееся на  $m^2$  (где  $m$  мы предполагаем положительным), то существует порядок форм с определителем  $D$ , произведенный из собственно примитивного порядка с определителем  $D/m^2$  (или два таких порядка, если  $D$  отрицательно, именно, один положительный и один отрицательный). Очевидно, что этому порядку будет принадлежать (положительная) форма  $(m, 0, -D/m)$ , которая по праву может рассматриваться как *простейшая* в нем (так же, как  $(-m, 0, D/m)$ , в случае отрицательного  $D$ , будет простейшей формой в отрицательном порядке). Если, кроме того,  $D/m^2 \equiv 1 \pmod{4}$ , то существует также порядок форм с определителем  $D$ , который произведен из несобственно примитивного порядка с определителем  $D/m^2$ , и которому будет принадлежать форма  $(2m, m, (m^2 - D)/2m)$ , являющаяся в нем простейшей. (Если  $D$  отрицательно, то снова имеется два порядка, и в отрицательном порядке в качестве простейшей следует рассматривать форму  $(-2m, -m, (D - m^2)/2m)$ ). Так, например, если мы хотим причислять сюда и случай, когда  $m = 1$ , то в четырех порядках форм с определителем 45 простейшими будут следующие формы:  $(1, 0, -45)$ ,  $(2, 1, -22)$ ,  $(3, 0, -15)$ ,  $(6, 3, -6)$ . В этом смысле надо понимать следующую задачу.

**Задача.** Пусть дана какая-нибудь форма  $f$  из порядка  $O$ ; нужно найти собственно примитивную (положительную) форму, при композиции которой с простейшей формой из  $O$  получается форма  $F$ .

**Решение.** Пусть форма  $F = (ma, mb, mc)$  произведена из примитивной формы  $f = (a, b, c)$ , определитель которой равен  $d$ , и предположим сначала, что  $f$  собственно примитивна. Заметим прежде всего, что если  $a$  не взаимно просто с  $2dm$ , то заведомо существуют другие, собственно эквивалентные форме  $(a, b, c)$  формы, которые этим свойством обладают. Действительно, согласно п. 228, существуют числа, взаимно простые с  $2dm$  и представляемые этой

формой; пусть таким числом является  $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ ; предположим (это допустимо), что  $\alpha, \gamma$  взаимно просты. Если тогда  $\beta, \delta$  выбраны так, что  $\alpha\delta - \beta\gamma = 1$ , то форма  $f$  при подстановке  $\alpha, \beta, \gamma, \delta$  переходит в форму  $(a', b', c')$ , которая собственно эквивалентна ей и обладает требуемым свойством. Но так как формы  $F$  и  $(a'm, b'm, c'm)$  также собственно эквивалентны, то легко видеть, что достаточно рассматривать тот случай, когда  $a$  взаимно просто с  $2dm$ . Тогда  $(a, bm, cm^2)$  будет собственно примитивной формой (так как если бы у  $a, 2bm, cm^2$  был общий делитель, то он содержался бы также и в  $2dm = 2b^2m - 2acm$ ) с тем же определителем, что и у формы  $F$ , и легко установить, что форма  $F$  при подстановке  $1, 0, -b, -cm; 0, m, a, bm$  переходит в произведение формы  $(m, 0, -dm)$ , — которая, если  $F$  не есть отрицательная форма, является простейшей формой порядка  $O$ , — и формы  $(a, bm, cm^2)$ , откуда, на основании критерия в четвертом замечании п. 235, вытекает, что  $F$  составлена из  $(m, 0, -dm)$  и  $(a, bm, cm^2)$ . Если же  $F$  — отрицательная форма, то она переходит в произведение простейшей формы  $(-m, 0, dm)$  из того же порядка и положительной формы  $(-a, bm, -cm^2)$  при подстановке  $1, 0, b, -cm; 0, -m, -a, bm$ , и потому составлена из них.

Если же  $f$  — несобственно примитивная форма, то можно считать, что  $a/2$  и  $2dm$  взаимно просты; действительно, если это свойство для формы  $f$  не имеет места, то можно найти собственно эквивалентную ей форму, которая этим свойством обладает. Но отсюда следует, что  $(a/2, bm, 2cm^2)$  будет собственно примитивной формой с тем же определителем, что и у формы  $F$ , и так же легко устанавливается, что  $F$  переходит в произведение форм

$$\left(\pm 2m, \pm m, \pm \frac{1}{2} (m - dm)\right), \left(\pm \frac{1}{2} a, bm, \pm 2cm^2\right)$$

при подстановке

$$1, 0, \frac{1}{2} (1 \mp b), -cm; \quad 0, \pm 2m, \pm \frac{1}{2} a, (b \pm 1) m,$$

где нужно брать нижние знаки, если  $F$  отрицательная форма, и верхние — в остальных случаях, и что тем самым  $F$  составлена из этих двух форм, первая из которых является простейшей в порядке  $O$ , а вторая — собственно примитивной (положительной) формой.

**Задача.** Пусть даны две формы  $F, f$  с одинаковым определителем  $D$ , которые принадлежат одному и тому же порядку  $O$ ; нужно найти собственно примитивную форму с определителем  $D$ , которая, будучи скомпонирована с  $f$ , порождает форму  $F$ .

**Решение.** Пусть  $\varphi$  — простейшая форма из порядка  $O$ ; далее, пусть  $\mathfrak{F}, \mathfrak{f}$  — собственно примитивные формы с определителем  $D$ , которые, будучи скомпонированы с  $\varphi$ , дают соответственно формы  $F, f$ ; наконец, пусть  $f'$  — собственно примитивная форма, которая будучи скомпонирована с  $\mathfrak{f}$ , порождает форму  $\mathfrak{F}$ . Тогда форма  $F$  будет составлена из трех форм  $\varphi, \mathfrak{f}, f'$ , или из двух форм  $f, f'$ .

Поэтому каждый класс из заданного порядка может рассматриваться как составленный из некоторого заданного класса этого же порядка и какого-нибудь собственно примитивного класса с тем же определителем.

**Для заданного определителя  
в отдельных родах из одного и того же порядка  
содержится по одинаковому числу классов**

**Теорема.** Для заданного определителя в отдельных родах из одного и того же порядка содержится по одинаковому числу классов.

**Доказательство.** Пусть роды  $G$  и  $H$  принадлежат одному и тому же порядку и пусть  $G$  состоит из  $n$  классов  $K, K', K'', \dots, K^{(n-1)}$ ; далее, пусть  $L$  — какой-нибудь класс из рода  $H$ . Найдем в соответствии с предыдущим пунктом собственно примитивный класс  $M$  с тем же определителем, при композиции которого с  $K$  получается класс  $L$ , и обозначим классы, получающиеся при композиции класса  $M$  с классами  $K', K'', \dots, K^{(n-1)}$  соответственно через  $L', L'', \dots, L^{(n-1)}$ . Тогда из последнего замечания в п. 249 следует, что все классы  $L, L', L'', \dots, L^{(n-1)}$  различны, и, согласно п. 248, все они принадлежат одному и тому же роду, т. е. роду  $H$ . Наконец, легко видеть, что  $H$  не может содержать других классов, кроме этих, так как каждый класс из рода  $H$  может рассматри-



ваться как составленный из  $M$  и некоторого другого класса того же определителя, который обязательно будет из рода  $G$ . Поэтому  $H$ , так же, как и  $G$ , содержит  $n$  различных классов.

**Сравниваются количества классов,  
содержащихся в отдельных родах из различных порядков**

253

Предыдущая теорема предполагает, что порядок один и тот же, и не может быть применена к различным порядкам. Так, например, для определителя  $-171$  имеется двадцать положительных классов, которые разбиваются на четыре порядка. В собственно примитивном порядке содержится два рода, каждый из которых охватывает по шесть классов; в несобственно примитивном порядке оба рода обладают четырьмя классами, каждый род — по два; в порядке, произведенном из собственно примитивного порядка с определителем  $-19$ , имеется только один род, который содержит три класса; наконец, порядок, произведенный из несобственно примитивного порядка с определителем  $-19$ , имеет только один род, состоящий из одного класса. Так же обстоит дело для отрицательных классов. Поэтому нужно постараться найти общий принцип, от которого зависит связь между числом классов в различных порядках. Предположим, что  $K, L$  — два класса из одного и того же (положительного) порядка  $O$  с определителем  $D$ , и  $M$  — собственно примитивный класс с тем же определителем, при композиции которого с  $K$  получается класс  $L$ ; такой класс  $M$ , согласно п. 251, всегда можно указать. В некоторых случаях  $M$  может быть единственным собственно примитивным классом, который, будучи скомпонирован с  $K$ , порождает  $L$ ; в других случаях может существовать несколько различных собственно примитивных классов, которые обладают этим свойством. Мы предположим для общности, что имеется  $r$  таких собственно примитивных классов  $M, M', M'', \dots, M^{(r-1)}$ , которые при композировании их по отдельности с  $K$ , дают один и тот же класс  $L$ , и обозначим их совокупность через  $W$ . Далее, пусть  $L'$  — другой (отличный от  $L$ ) класс из порядка  $O$ , и  $N'$  — собственно примитивный класс с определителем  $D$ , который, будучи скомпонирован

с  $L$ , порождает  $L'$ ; совокупность классов  $N' + M$ ,  $N' + M'$ ,  $N' + M''$ , ...,  $N' + M^{(r-1)}$  (которые все собственно примитивны и отличны один от другого) обозначим через  $W'$ . Тогда очевидно, что  $K$ , будучи скомпонировано с любым классом из  $W'$ , дает  $L'$ , откуда следует, что  $W$  и  $W'$  не имеют общих классов; кроме того, без труда доказывается, что не существует собственно примитивных, не содержащихся в совокупности  $W'$  классов, которые, будучи скомпонованы с  $K$ , давали бы  $L'$ . Таким же образом убеждаемся, что если  $L''$  — другой, отличный от классов  $L$ ,  $L'$  класс из порядка  $O$ , то имеется  $r$  собственно примитивных классов, отличных как один от другого, так и от классов из  $W$ ,  $W'$ , которые при композиции их по отдельности с  $K$  дают  $L''$ , и так же обстоит дело со всеми классами из порядка  $O$ . Так как, однако, каждый собственно примитивный (положительный) класс с определителем  $D$ , будучи скомпонован с  $K$ , дает класс из порядка  $O$ , то отсюда легко получается, что если количество всех классов в порядке  $O$  равно  $n$ , то количество всех собственно примитивных (положительных) классов с тем же определителем равно  $rn$ . Мы получаем поэтому *общее правило*: если  $K$ ,  $L$  обозначают какие-нибудь два класса из порядка  $O$ , и  $r$  — число различных собственно примитивных классов с тем же определителем, которые при композиции их по отдельности с  $K$  порождают  $L$ , то число всех классов в собственно примитивном (положительном) порядке в  $r$  раз больше, чем число всех классов в порядке  $O$ .

Так как классы  $K$ ,  $L$  и порядка  $O$  могут предполагаться совершенно произвольными, то можно брать и идентичные классы, причем будет целесообразно воспользоваться тем классом, в котором содержится простейшая форма из этого порядка. Поэтому, если взять этот класс вместо  $K$  и  $L$ , то вопрос сводится к тому, чтобы указать все собственно примитивные классы, которые при композиции с  $K$  снова порождают  $K$ . Путь к этому пролагается теоремой следующего пункта.

**Теорема.** Если  $F = (A, B, C)$  — простейшая форма из порядка  $O$  с определителем  $D$ , и  $f = (a, b, c)$  — собственно примитивная

форма с тем же определителем, то число  $A^2$  представляется этой формой  $f$ , если  $F$  получается при композиции форм  $f$ ,  $F$ , и, обратно, если  $F$  составлена из себя самой и  $f$ , то  $A^2$  представляется формой  $f$ .

**Доказательство.** I. Если  $F$  переходит в произведение  $fF$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$ , то, согласно п. 235, мы имеем

$$A(aq''^2 - 2bqq'' + cq^2) = A^3, \text{ и потому } A^2 = aq''^2 - 2bqq'' + cq^2.$$

II. Предполагая, что  $A^2$  может быть представлено формой  $f$ , обозначим значения неизвестных, при которых это достигается, через  $q'', -q$ , т. е. будем считать, что  $A^2 = aq''^2 - 2bqq'' + cq^2$ , и положим

$$\begin{aligned} q''a - q(b + B) &= Ap, & -qC &= Ap', & q''(b - B) - qc &= Ap'', \\ -q''C &= Ap''', & q''a - q(b - B) &= Aq', & q''(b + B) - qc &= Aq'''. \end{aligned}$$

Тогда легко показать, что  $F$  переходит в произведение  $fF$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$  и потому составлена из  $f$  и  $F$ , если только все числа  $p, p', \dots$  целые. Но, по определению простейшей формы,  $B$  или равно 0, или равно  $A/2$ , поэтому число  $2B/A$  целое; отсюда же следует, что и  $C/A$  целое число. Поэтому целыми числами будут  $q' - p, p', q''' - p'', p'''$ , и потому остается только показать, что  $p$  и  $p''$  целые. Но

$$p^2 + \frac{2pqB}{A} = a - \frac{q^2C}{A}, \quad p''^2 + \frac{2p''q''B}{A} = c - \frac{q''^2C}{A};$$

если поэтому  $B = 0$ , то

$$p^2 = a - \frac{q^2C}{A}, \quad p''^2 = c - \frac{q''^2C}{A},$$

и тем самым числа  $p$  и  $p''$  целые. Если же  $B = \frac{A}{2}$ , то

$$p^2 + pq = a - \frac{q^2C}{A}, \quad p''^2 + p''q'' = c - \frac{q''^2C}{A},$$

откуда так же легко получается, что и в этом случае  $p$  и  $p''$  целые числа. Из этого следует, что  $F$  составлена из  $f$  и  $F$ .

Проблема теперь свелась к тому, что нужно определить все собственно примитивные классы с определителем  $D$ , формами из которых представляется число  $A^2$ . Очевидно, что  $A^2$  представляется каждой формой, первый член которой равен или  $A^2$ , или квадрату какого-нибудь делителя  $A$ ; наоборот, если  $A^2$  представляется формой  $f$  при значениях неизвестных  $\alpha e$ ,  $\beta e$ , наибольший общий делитель которых равен  $e$ , то форма  $f$  при подстановке  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta$  будет переходить в форму, первый член которой есть  $A^2/e^2$ , и которая будет собственно эквивалентна форме  $f$ , если  $\alpha\delta - \beta\gamma = 1$ . Из этого вытекает, что в каждом классе, формами которого может быть представлено  $A^2$ , находятся формы, у которых первый член есть или  $A^2$ , или квадрат делителя числа  $A$ . Итак, дело сводится к тому, чтобы определить все собственно примитивные классы с определителем  $D$ , в которых имеются такие формы, и это достигается следующим образом. Пусть  $a$ ,  $a'$ ,  $a''$ , ... все положительные делители  $A$ ; найдем все значения выражения  $\sqrt{D} \pmod{a^2}$ , которые лежат между 0 и  $a^2 - 1$  включительно, и которые пусть равны  $b$ ,  $b'$ ,  $b''$ , ..., и положим

$$b^2 - D = a^2c, \quad b'^2 - D = a'^2c', \quad b''^2 - D = a''^2c'', \quad \dots;$$

далее, обозначим совокупность форм  $(a^2, b, c)$ ,  $(a^2, b', c')$ , ... через  $V$ . Тогда легко видеть, что в каждом классе с определителем  $D$ , в котором встречается форма, первый член которой равен  $a^2$ , должна содержаться также какая-нибудь форма из  $V$ . Аналогичным образом получим все формы с определителем  $D$ , первый член которых есть  $a'^2$ , а средний член расположен между 0 и  $a'^2 - 1$  включительно, и обозначим совокупность их через  $V'$ . Точно так же пусть  $V''$  — совокупность аналогичных форм, первый член которых есть  $a''^2$  и т. д. Из форм  $V$ ,  $V'$ ,  $V''$ , ... удалим те формы, которые не являются собственно примитивными, остальные разобьем на классы и в каждом отдельном классе оставим только по одной из них, если случайно окажется несколько принадлежащих одному и тому же классу. Таким способом мы получим все искомые классы, и число их будет относиться к единице как число всех собственно примитивных (положительных) классов относится к числу классов в порядке  $O$ .

**Пример.** Пусть  $D = -531$  и  $O$  — произведенный из несобственно примитивного порядка с определителем  $-59$  положительный порядок, простейшей формой в котором является  $(6, 3, 90)$ , т. е.  $A=6$ . Здесь  $a, a', a'', a'''$  равны соответственно  $1, 2, 3, 6$ . Совокупность  $V$  содержит форму  $(1, 0, 531)$ , совокупность  $V'$  — формы  $(4, 1, 133)$ ,  $(4, 3, 135)$ , совокупность  $V''$  — формы  $(9, 0, 59)$ ,  $(9, 3, 60)$ ,  $(9, 6, 63)$ , наконец, совокупность  $V'''$  содержит формы  $(36, 3, 15)$ ,  $(36, 9, 17)$ ,  $(36, 15, 21)$ ,  $(36, 21, 27)$ ,  $(36, 27, 35)$ ,  $(36, 33, 45)$ . Однако из этих двенадцати форм шесть нужно отбросить, а именно, из совокупности  $V''$  — вторую и третью, а из  $V'''$  — первую, третью, четвертую и шестую, так как все эти формы являются произведенными; относительно же оставшихся форм можно убедиться, что все они принадлежат различным классам. Действительно, число собственно примитивных (положительных) классов с определителем  $-531$  равно  $18$ , а число несобственно примитивных (положительных) классов с определителем  $-59$  (т. е. число произведенных из них классов с определителем  $-531$ ) равно  $3$ ; таким образом, первое число относится ко второму как  $6$  к  $1$ .

## 256

Это решение делается еще более ясным после следующих общих замечаний.

I. Если порядок  $O$  произведен из собственно примитивного порядка, то  $A^2$  входит в  $D$ ; если же порядок  $O$  несобственно примитивный или произведен из несобственно примитивного порядка, то  $A$  четно,  $D$  делится на  $A^2/4$ , и частное  $\equiv 1 \pmod{4}$ . Поэтому квадрат каждого делителя числа  $A$  будет входить или в  $D$ , или по крайней мере в  $4D$ , причем в последнем случае частное всегда будет  $\equiv 1 \pmod{4}$ .

II. Если  $a^2$  входит в  $D$ , то всевозможными значениями выражения  $\sqrt{D} \pmod{a^2}$ , которые лежат между  $0$  и  $a^2 - 1$ , будут следующие:  $0, a, 2a, \dots, a^2 - a$ , и потому число форм  $V$  есть  $a$ . Но среди них будет лишь столько собственно примитивных, сколько имеется в ряду

$$\frac{D}{a^2}, \frac{D}{a^2} - 1, \frac{D}{a^2} - 4, \dots, \frac{D}{a^2} - (a - 1)^2$$

чисел, которые не имеют общих делителей с  $a$ . Если  $a = 1$ , то  $V$  будет состоять только из одной формы  $(1, 0, -D)$ , которая всегда собственно примитивна. Если  $a = 2$  или есть степень числа 2, то половина указанных  $a$  чисел будут четными, а остальные нечетными; поэтому в  $V$  будет содержаться  $a/2$  собственно примитивных форм. Если  $p$  есть какое-нибудь другое простое число или степень простого числа, то нужно различать три случая, именно: все эти  $a$  чисел будут взаимно просты с  $a$ , и потому все формы из  $V$  будут собственно примитивны, если  $D/a^2$  не делится на  $p$  и одновременно не является квадратичным вычетом по модулю  $p$ ; если же  $p$  входит в  $D/a^2$ , то в  $V$  имеется  $(p-1)a/p$  собственно примитивных форм; наконец, если  $D/a^2$  есть не делящийся на  $p$  квадратичный вычет по модулю  $p$ , то в  $V$  имеется  $(p-2)a/p$  собственно примитивных форм. Все это может быть доказано без труда. Если же положить вообще  $a = 2^v p^\pi q^\chi r^\rho \dots$ , где  $p, q, r, \dots$  обозначают различные нечетные простые числа, то количество собственно примитивных форм в  $V$  равно  $NPQR\dots$ , где нужно положить

$$N = 1 \quad (\text{если } v = 0) \text{ или } N = 2^{v-1} \quad (\text{если } v > 0),$$

$$P = p^\pi \quad (\text{если } D/a^2 \text{ является квадратичным невычетом по модулю } p),$$

или

$$P = (p-1)p^{\pi-1} \quad (\text{если } D/a^2 \text{ делится на } p), \text{ или}$$

$$P = (p-2)p^{\pi-1} \quad (\text{если } D/a^2 \text{ есть не делящийся на } p \text{ квадратичный вычет по модулю } p),$$

а числа  $Q, R, \dots$  определяются соответственно из  $q, r, \dots$  так же, как  $P$  из  $p$ .

III. Если  $a^2$  не входит в  $D$ , то  $4D/a^2$  — число целое и  $\equiv 1 \pmod{4}$ ; значения выражения  $\sqrt{D} \pmod{a^2}$  суть:  $a/2, 3a/2, 5a/2, \dots, a^2 - \frac{1}{2}a$ ; поэтому количество форм в  $V$  равно  $a$ , и из них будет столько собственно примитивных, сколько среди чисел

$$\frac{D}{a^2} - \frac{1}{4}, \frac{D}{a^2} - \frac{9}{4}, \frac{D}{a^2} - \frac{25}{4}, \dots, \frac{D}{a^2} - \left(a - \frac{1}{2}\right)^2$$

имеется взаимно простых с  $a$ . Если  $\frac{4D}{a^2} \equiv 1 \pmod{8}$ , то все эти числа четны, и потому в  $V$  нет собственно примитивных форм; если же  $\frac{4D}{a^2} \equiv 5 \pmod{8}$ , то все эти числа нечетные, и потому в  $V$  все формы

будут собственно примитивными, если  $a$  равно 2 или есть степень числа 2, вообще же в этом случае в  $V$  будет столько собственно примитивных форм, сколько среди этих чисел имеется не делящихся ни на один простой делитель числа  $a$ . Если  $a = 2^v p^\pi q^\chi r^\rho \dots$ , то это количество равно  $NRQR \dots$ , где нужно положить  $N = 2^v$ , а остальные  $P, Q, R, \dots$  выводятся из  $p, q, r, \dots$  таким же образом, как в предыдущем случае.

IV. Итак, этим способом можно определить количество собственно примитивных форм в  $V, V', V'', \dots$ ; для суммы всех этих количеств без труда находится следующее *общее правило*. Если  $A = 2^v \mathfrak{A}^\alpha \mathfrak{B}^\beta \mathfrak{C}^\gamma \dots$ , где  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  обозначают различные нечетные простые числа, то общее количество всех собственно примитивных форм в  $V, V', V'', \dots$  равно  $\frac{A n a b c \dots}{2^v \mathfrak{A} \mathfrak{B} \mathfrak{C} \dots}$ , где нужно положить

$$\begin{aligned} n &= 1 && \left( \text{если } \frac{4D}{A^2} \equiv 1 \pmod{8} \right), \text{ или} \\ n &= 2 && \left( \text{если } \frac{D}{A^2} \text{ есть целое число} \right), \text{ или} \\ n &= 3 && \left( \text{если } \frac{4D}{A^2} \equiv 5 \pmod{8} \right), \text{ далее,} \\ \alpha &= \mathfrak{A} && \left( \text{если } \mathfrak{A} \text{ входит в } \frac{4D}{A^2} \right), \text{ или} \\ \alpha &= \mathfrak{A} \pm 1 && \left( \text{если } \mathfrak{A} \text{ не входит в } \frac{4D}{A^2}, \text{ причем нужно брать верхний} \right. \\ &&& \left. \text{или нижний знак в зависимости от того, является} \right. \\ &&& \left. \text{ли } 4D/A^2 \text{ квадратичным невычетом или вычетом по} \right. \\ &&& \left. \text{модулю } \mathfrak{A} \right); \end{aligned}$$

и  $b, c, \dots$  выводятся из  $\mathfrak{B}, \mathfrak{C}, \dots$  так же, как  $\alpha$  из  $\mathfrak{A}$ . Ради краткости мы не будем излагать здесь доказательство более подробно.

V. Что же касается *числа классов*, которые дают собственно примитивные формы из  $V, V', V'', \dots$ , то здесь нужно различать *следующие три случая*.

Во-первых, если число  $D$  отрицательно, то отдельные собственно примитивные формы в  $V, V', \dots$  образуют каждая особый класс, т. е. число искомых классов выражается формулой, указанной в предыдущем замечании, за исключением двух случаев, именно, когда  $4D/A^2$  или  $= -4$ , или  $= -3$ , т. е. когда  $D$  или  $= -A^2$ , или  $= -\frac{3}{4}A^2$ . Для того, чтобы доказать эту теорему, нужно, очевидно,

только показать, что не может случиться того, что две различные формы из  $V, V', V'', \dots$  собственно эквивалентны. Если предположить, что  $(h^2, i, k), (h'^2, i', k')$  — две различные собственно примитивные формы из  $V, V', V'', \dots$ , которые принадлежат одному и тому же классу, и что первая переходит во вторую при собственной подстановке  $\alpha, \beta, \gamma, \delta$ , так что имеют место равенства

$$\alpha\delta - \beta\gamma = 1, \quad h^2\alpha^2 + 2i\alpha\gamma + k\gamma^2 = h'^2, \quad h^2\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i',$$

то отсюда легко следует: *во-первых*, что  $\gamma$  заведомо не равно 0 (действительно, в противном случае было бы  $\alpha = \pm 1$ ,  $h^2 = h'^2$ ,  $i' \equiv i \pmod{h^2}$ , и потому заданные формы были бы идентичны, что противоречит предположению); *во-вторых*, что  $\gamma$  делится на наибольший общий делитель чисел  $h, h'$  (действительно, если положить этот делитель равным  $r$ , то он, очевидно, входит также в  $2i, 2i'$ , но взаимно прост с  $k$ ; кроме того,  $r^2$  входит в  $h^2k - h'^2k' = i^2 - i'^2$ , откуда легко следует, что  $r$  входит также в  $i - i'$ ; но  $\alpha i' - \beta h'^2 = \alpha i + \gamma k$ , и потому  $\gamma k$ , а значит, и  $\gamma$  делятся на  $r$ ); *в-третьих*, что  $(\alpha h^2 + \gamma i)^2 - D\gamma^2 = h^2 h'^2$ . Поэтому, если положить  $\alpha h^2 + \gamma i = rp$ ,  $\gamma = rq$ , то  $p, q$  будут целыми числами, причем второе не равно 0, и  $p^2 - Dq^2 = \frac{h^2 h'^2}{r^2}$ . Но  $h^2 h'^2 / r^2$  является наименьшим числом, делящимся одновременно на  $h^2$  и  $h'^2$ , и потому также входит в  $A^2$ , а тем самым и в  $4D$ ; следовательно,  $4Dr^2 / h^2 h'^2$  есть целое (отрицательное) число, и если положить его равным  $-e$ , то будет  $p^2 - Dq^2 = -\frac{4D}{e}$  или  $4 = \left(\frac{2rp}{hh'}\right)^2 + eq^2$ . В этом равенстве член  $(2rp / hh')^2$ , будучи квадратом, меньшим 4, обязательно или равен 0, или равен 1. В первом случае  $eq^2 = 4$ , и  $D = -\left(\frac{hh'}{rq}\right)^2$ , откуда следует, что отношение  $4D / A^2$  есть взятый с отрицательным знаком квадрат и потому заведомо не сравнимо с  $1 \pmod{4}$ , так что  $O$  не может быть ни несобственно примитивным, ни произведенным из несобственно примитивного порядка порядком. Поэтому  $D / A^2$  есть целое число, откуда легко следует, что  $e$  делится на 4,  $q^2 = 1$ ,  $D = -\left(\frac{hh'}{r}\right)^2$  и  $A^2 / D$  — тоже целое число. Следовательно, обязательно  $D = -A^2$  или  $\frac{D}{A^2} = -1$ , что приводит к *первому исключенному случаю*. Во



втором случае  $eq^2 = 3$ , так что  $e = 3$  и  $4D = -3\left(\frac{hh'}{r}\right)^2$ . Поэтому  $3\left(\frac{hh'}{rA}\right)^2$  есть целое число, которое может быть равно только 3, так как, будучи умноженным на целочисленный квадрат  $\left(\frac{rA}{hh'}\right)^2$ , оно дает число 3. Следовательно,  $4D = -3A^2$  или  $D = -\frac{3}{4}A^2$ , что представляет собой *второй исключенный случай*. Во всех же остальных случаях все собственно примитивные формы из  $V, V', V'', \dots$  будут, таким образом, принадлежать различным классам. Для исключенных случаев достаточно сообщить результаты нетрудного, но ради краткости опускаемого здесь исследования. Именно, в первом случае среди собственно примитивных форм из  $V, V', V'', \dots$  в одном и том же классе каждый раз оказывается по две, а во втором случае по три формы, так что число всех искомых классов в первом случае равно половине, а во втором — третьей части выражения, приведенного в предыдущем замечании.

Во-вторых, если  $D$  положительный квадрат, то отдельные собственно примитивные формы из  $V, V', V'', \dots$  все без исключения будут образовывать особые классы. Действительно, если предположить, что  $(h^2, i, k), (h'^2, i', k')$  — две такие различные собственно эквивалентные формы, и что первая переходит во вторую при собственной подстановке  $\alpha, \beta, \gamma, \delta$ , то очевидно, что все сделанные в предыдущем случае заключения, в которые не входило предположение, что  $D$  отрицательно, остаются в силе и здесь. Поэтому если  $p, q, r$  обозначают здесь то же, что и там, то и здесь  $4Dr^2/h^2h'^2$  будет целым числом, но уже не отрицательным, а положительным и, кроме того, — квадратным, и если положить его равным  $g^2$ , то  $\left(\frac{2rp}{hh'}\right)^2 - g^2q^2 \equiv 4$ . Это, однако, невозможно, так как разность двух квадратов не может быть равна 4. Поэтому предположение не может быть правильным.

Для третьего случая, однако, когда  $D$  является положительным неквадратным числом, мы до сих пор еще не обладаем общим правилом для того, чтобы сравнивать число собственно примитивных форм в  $V, V', V'', \dots$  с числом различных получающихся отсюда классов. Мы можем только утверждать, что второе или равно первому, или является его делителем; мы обнаружили даже своеобразную

связь между отношением этих чисел и наименьшими удовлетворяющими уравнению  $t^2 - Du^2 = A^2$  значениями  $t, u$ , излагать которую здесь было бы слишком долго; но можно ли всегда узнать это отношение только по числам  $D, A$  (как в предыдущих случаях), мы сказать определенно не можем. Здесь мы дадим несколько примеров, количество которых каждый может легко умножить. Для  $D = 13, A = 2$  число собственно примитивных форм в  $V, \dots$  равно 3, и все они эквивалентны, т. е. образуют только один класс; для  $D = 37, A = 2$  в  $V, \dots$  также имеется три собственно примитивных формы, которые принадлежат трем различным классам; для  $D = 588, A = 7$  в  $V, \dots$  имеется восемь собственно примитивных форм, которые образуют четыре класса; для  $D = 867, A = 17$  в  $V, \dots$  встречается восемнадцать собственно примитивных форм, и для  $D = 1445, A = 17$  столько же, но для первого определителя они распадаются на два, а для второго — на шесть классов.

VI. Из применения этой общей теории к тому случаю, когда  $O$  есть несобственно примитивный порядок, следует, что число содержащихся в этом порядке классов относится к числу всех классов в собственно примитивном порядке как 1 к числу различных собственно примитивных классов, которые образуют следующие три формы:  $(1, 0, -D), (4, 1, (1-D)/4), (4, 3, (9-D)/4)$ . Если  $D \equiv 1 \pmod{8}$ , то отсюда получается только один класс, так как в этом случае вторая и третья формы несобственно примитивны; если же  $D \equiv 5 \pmod{8}$ , то все эти три формы будут собственно примитивны, и потому при отрицательном  $D$  дадут столько же различных классов, за исключением единственного случая  $D = -3$ , когда они образуют только один класс; наконец, случай, когда  $D$  положительно (вида  $8n + 5$ ), относится к тем, для которых общего правила еще не известно. Однако мы можем утверждать, что в этом случае указанные три формы принадлежат или к трем различным классам, или к одному, но никогда не к двум. Действительно, легко убедиться, что если формы  $(1, 0, -D), (4, 1, (1-D)/4), (4, 3, (9-D)/4)$  принадлежат соответственно классам  $K, K', K''$ , то  $K + K' = K', K' + K' = K''$ , и потому, если предположить идентичными  $K$  и  $K'$ , то будут идентичными также  $K'$  и  $K''$ ; точно так же, если предположить идентичными  $K$  и  $K''$ , то и  $K'$  и  $K''$  тоже будут идентичными;

наконец, так как  $K' + K'' = K$ , то из предположения об идентичности  $K'$  и  $K''$  следует также идентичность  $K$  и  $K''$ . Отсюда получается, что или все три класса  $K, K', K''$  различны, или все три совпадают. Например, среди чисел до 1000 всего будет 125 чисел вида  $8n + 5$ , из которых для 31 определителя имеет место первый случай, т. е. число классов в собственно примитивном порядке втрое больше, чем в несобственно примитивном, именно, для 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573, 677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997; для остальных 94 определителей имеет место второй случай, т. е. для них число классов в обоих порядках одинаково.

VII. Едва ли нужно говорить, что при помощи этого исследования могут сравниваться между собой не только число классов в различных порядках одного и того же определителя, но что оно применимо также к любым различным определителям, которые относятся один к другому как квадраты. Именно, если  $O$  обозначает какой-нибудь порядок определителя  $dm^2$ , а  $O'$  — порядок определителя  $dm'^2$ , то  $O$  можно сравнить с собственно примитивным порядком с определителем  $dm^2$ , а его — с порядком, произведенным из собственно примитивного порядка с определителем  $d$ , или, что в отношении числа классов сводится к тому же, — с самим этим последним порядком, и с ним же можно точно так же сравнить порядок  $O'$ .

### О числе двусторонних классов

257

Среди всех классов в заданном порядке с заданным определителем в особенности требуют подробного исследования двусторонние классы, и определение числа таких классов проложит нам путь ко многому другому. Достаточно, однако, определить указанное число только для собственно примитивного порядка, так как остальные случаи легко могут быть сведены к этому. Эту задачу мы выполним так: сначала покажем, как находить все собственно примитивные двусторонние формы  $(A, B, C)$  с заданным определителем  $D$ , у которых или  $B = 0$ , или  $B = \frac{1}{2}A$ , а затем, как, зная их число, найти число всех собственно примитивных двусторонних форм с определителем  $D$ .

I. Очевидно, мы найдем все собственно примитивные формы  $(A, 0, C)$  с определителем  $D$ , если возьмем за  $A$  отдельные делители (как положительные, так и отрицательные) числа  $D$ , для которых  $C = -\frac{D}{A}$  взаимно просто с  $A$ . Поэтому если  $D = 1$ , таких форм имеется две:  $(1, 0, -1)$ ,  $(-1, 0, 1)$ ; столько же их будет, если  $D = -1$ , именно  $(1, 0, 1)$ ,  $(-1, 0, -1)$ ; если  $D$  простое число или степень простого числа (будь то с положительным или отрицательным знаком), то их имеется четыре:  $(1, 0, -D)$ ,  $(-1, 0, D)$ ,  $(D, 0, -1)$ ,  $(-D, 0, 1)$ . Вообще же, если  $D$  делится на  $n$  различных простых чисел (к которым здесь должно быть причислено и 2), то всего имеется  $2^{n+1}$  таких форм. Именно, если положить  $D = \pm PQR \dots$ , где  $P, Q, R, \dots$  обозначают различные простые числа или степени таковых, количество которых равно  $n$ , то значениями  $A$  будут числа  $1, P, Q, R, \dots$  и произведения любого количества этих чисел; количество этих значений равно  $2^n$ ; однако, его нужно удвоить, так как отдельным значениям нужно придавать как положительные, так и отрицательные знаки.

II. Подобным же образом оказывается, что все собственно примитивные формы  $(2B, B, C)$  с определителем  $D$  получаются, если за  $B$  брать все делители (как положительные, так и отрицательные) числа  $D$ , для которых  $C = \frac{1}{2}\left(B - \frac{D}{B}\right)$  будет целым числом, взаимно простым с  $2B$ . Так как при этом  $C$  обязательно нечетно и потому  $C^2 \equiv 1 \pmod{8}$ , то из  $D = B^2 - 2BC = (B - C)^2 - C^2$  следует, что  $D$  или  $\equiv 3 \pmod{4}$ , если  $B$  нечетно, или  $\equiv 0 \pmod{8}$ , если  $B$  четно; поэтому, если  $D$  сравнимо по модулю 8 с одним из чисел 1, 2, 4, 5, 6, 7, то форм такого вида нет. Если  $D \equiv 3 \pmod{4}$ , то  $C$  целое и нечетное, какой бы делитель числа  $D$  ни брать за  $B$ ; а для того чтобы  $C$  не имело общих делителей с  $2B$ , нужно брать такие  $B$ , чтобы  $D/B$  было взаимно просто с  $B$ . Поэтому для  $D = -1$  мы получаем две формы  $(2, 1, 1)$ ,  $(-2, -1, -1)$ , а вообще легко убедиться, что если количество всех входящих в  $D$  простых чисел равно  $n$ , то всего имеется  $2^{n+1}$  форм. Если  $D$  делится на 8, то  $C$  будет целым числом, если за  $B$  брать какой-нибудь четный делитель числа  $D/2$ ; а другое условие, именно, что  $C = \frac{1}{2}B - \frac{D}{2B}$  должно быть взаимно просто с  $2B$ , удовлетворяется,

во-первых, тем что в качестве  $B$  берутся все четные, но не делящиеся на 4 делители числа  $D$ , для которых  $D/B$  не имеет с  $B$  общих делителей и количество которых (принимая во внимание возможность различных знаков) равно  $2^{n+1}$ , где  $n$  обозначает количество различных нечетных простых делителей числа  $D$ ; во-вторых, тем, что в качестве  $B$  берутся все делящиеся на 4 делители числа  $D/2$ , для которых  $D/2B$  взаимно просто с  $B$  и количество которых тоже равно  $2^{n+1}$ , так что всего в этом случае мы получаем  $2^{n+2}$  таких форм. Именно, если, положить  $D = \pm 2^\mu PQR \dots$ , где  $\mu$  обозначает некоторый показатель степени, больший чем 2, а  $P, Q, R, \dots$  — различные нечетные простые числа (или степени таких чисел), количество которых равно  $n$ , то и в качестве  $B/2$  и в качестве  $D/2B$  можно брать значения 1,  $P, Q, R, \dots$  и произведения любого количества этих чисел как с положительным, так и с отрицательным знаком.

Из всего этого мы выводим, что если считать  $D$  делящимся на  $n$  различных нечетных простых чисел (где нужно положить  $n = 0$ , если  $D = \pm 1$  или  $= \pm 2$ , или равно степени числа 2), то количество всех собственно примитивных форм  $(A, B, C)$ , у которых  $B$  или равно 0, или равно  $A/2$ , равно  $2^{n+1}$ , если  $D \equiv 1$  или  $\equiv 5 \pmod{8}$ , равно  $2^{n+2}$ , если  $D \equiv 2, 3, 4, 6$  или  $7 \pmod{8}$ , наконец, равно  $2^{n+3}$ , если  $D \equiv 0 \pmod{8}$ . Если сравнить это число с тем, которое мы указали в п. 231 для количества всех возможных характеров примитивных форм с определителем  $D$ , то можно заметить, что первое во всех случаях в точности вдвое больше второго. Впрочем, ясно, что если  $D$  отрицательно, то среди указанных форм всегда имеются столько же положительных, сколько и отрицательных.

Очевидно, что все полученные в предыдущем пункте формы принадлежат двусторонним классам, и, обратно, в каждом двустороннем собственно примитивном классе с определителем  $D$  должна содержаться по меньшей мере одна из таких форм; действительно, в таком классе заведомо встречаются двусторонние формы, и каждой собственно примитивной двусторонней форме  $(a, b, c)$  с определителем  $D$  эквивалентна какая-нибудь из форм предыдущего пункта,

именно,

$$\text{или } \left(a, 0, -\frac{D}{a}\right), \text{ или } \left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a}\right),$$

в зависимости от того, сравнимо ли  $b$  с 0 или  $\frac{1}{2}a \pmod{a}$ . Задача поэтому сводится к тому, чтобы определить, сколько различных классов образуют эти формы.

Если среди форм предыдущего пункта фигурирует форма  $(a, 0, c)$ , то среди них будет и форма  $(c, 0, a)$ , которая будет всегда отлична от первой, кроме единственного случая, когда  $a = c = \pm 1$ , и потому  $D = -1$ ; этот случай мы пока не будем принимать во внимание. Но так как эти формы, очевидно, принадлежат одному и тому же классу, то из них нужно оставить только одну, причем мы отбросим ту, у которой первый член больше третьего; случай, когда  $a = -c = \pm 1$  или  $D = 1$ , мы тоже оставим в стороне. Таким образом, мы можем разбить все формы  $(A, 0, C)$  на две части, причем из каждой двух все время будем оставлять одну, и во всех оставшихся будет  $A < \sqrt{\pm D}$ .

Аналогично, если среди форм предыдущего пункта фигурирует форма  $(2b, b, c)$ , то среди них будет находиться также и форма

$$(4c - 2b, 2c - b, c) = \left(-\frac{2D}{b}, -\frac{D}{b}, c\right),$$

которая собственно эквивалентна первой и отлична от нее, за исключением случая, когда  $c = b = \pm 1$  или  $D = -1$ , рассмотрение которого мы отложим. Из этих двух форм нужно оставить только ту, у которой первый член меньше, чем первый член другой (быть равными по величине, но иметь различные знаки они в этом случае не могут); отсюда вытекает, что также и все формы  $(2B, B, C)$  могут быть сведены к половине их, если из каждой двух все время сохранять только одну, и что у оставшихся форм  $B < \frac{D}{B}$ , т. е.  $B < \sqrt{\pm D}$ . Таким образом, из всех форм предыдущего пункта остается только половина форм, совокупность которых мы обозначим через  $W$ , и остается только показать, сколько из них может получиться различных классов. Между прочим, ясно, что в случае,

когда  $D$  отрицательно, в  $W$  содержится столько же положительных форм, сколько и отрицательных.

I. Если  $D$  отрицательно, то отдельные формы в  $W$  будут принадлежать различным классам. Действительно, все формы  $(A, 0, C)$  приведенные, и точно так же среди форм  $(2B, B, C)$  все приведенные, за исключением тех, у которых  $C < 2B$ . Но у такой формы  $2C < 2B + C$ , и потому (так как  $B < \frac{D}{B}$  т. е.  $B < 2C - B$ , и потому  $2B < 2C$ , т. е.  $B < C$ )  $2C - 2B < C$  и  $C - B < \frac{1}{2}C$ , и тем самым форма  $(C, C - B, C)$ , которая, очевидно, эквивалентна первой, является приведенной. Таким образом, мы имеем столько же приведенных форм, сколько имеется форм в  $W$ , и так как легко видеть, что среди них нет ни идентичных, ни противоположных (кроме случая  $C - B = 0$ , когда  $B = C = \pm 1$  и потому  $D = -1$ , который мы уже отложили), то все формы будут принадлежать различным классам. Отсюда следует, что число всех двусторонних собственно примитивных классов с определителем  $D$  равно числу форм в  $W$ , или половине числа форм предыдущего пункта; в исключенном же случае  $D = -1$  дело обстоит так же вследствие того, что имеется два класса, одному из которых принадлежат формы  $(1, 0, 1)$ ,  $(2, 1, 1)$ , а другому — формы  $(-1, 0, -1)$ ,  $(-2, -1, -1)$ . Таким образом, вообще, для отрицательного определителя число всех двусторонних собственно примитивных классов равно числу всех возможных характеров примитивных форм этого определителя; число же положительных двусторонних собственно примитивных классов равно половине указанного числа.

II. Если  $D$  — положительный квадрат  $h^2$ , то без труда доказывается, что отдельные формы из  $W$  принадлежат различным классам; однако, в этом случае мы можем получить решение проблемы еще быстрее следующим образом. Так как, согласно п. 210, в каждом двустороннем собственно примитивном классе с определителем  $h^2$  (и ни в каких других) содержится одна приведенная форма  $(a, h, 0)$ , у которой  $a$  является значением выражения  $\sqrt{1} \pmod{2h}$  и лежит между 0 и  $2h - 1$  включительно, то ясно, что собственно примитивных двусторонних классов с определителем  $h^2$  существует столько же, сколько значений имеет это выражение. Но из п. 105 легко



получается, что число этих значений равно  $2^n$ , или  $2^{n+1}$ , или  $2^{n+2}$ , в зависимости от того, является ли  $h$  нечетным, или четным, но не делящимся на 4, или делящимся на 4, т. е. в зависимости от того,  $D \equiv 1$ , или  $\equiv 4$ , или  $\equiv 0 \pmod{8}$ , причем  $n$  обозначает число нечетных простых делителей  $h$  или  $D$ . Отсюда следует, что число двусторонних собственно примитивных классов всегда равно половине числа всех указанных в предыдущем пункте форм, т. е. равно числу форм в  $W$ , т. е. равно числу всех возможных характеров

III. Если  $D$  — положительное число, не являющееся квадратом, то произведем из отдельных форм  $(A, B, C)$ , которые содержатся в  $W$ , новые формы  $(A, B', C')$ , полагая  $B' \equiv B \pmod{A}$ , причем  $B'$  заключено между границами  $\sqrt{D}$  и  $\sqrt{D} \mp A$  (где берется верхний или нижний знак в зависимости от того, положительно  $A$  или отрицательно), и  $C' = \frac{B'^2 - D}{A}$ ; совокупность этих новых форм обозначим через  $W'$ . Очевидно, что эти формы будут собственно примитивными двусторонними формами с определителем  $D$ , различными между собой; кроме того, все эти формы приведены. Действительно, если  $A < \sqrt{D}$ , то, очевидно,  $B' < \sqrt{D}$  и положительно; кроме того,  $B' > \sqrt{D} \mp A$ , и потому  $A > \sqrt{D} - B'$ , и тем самым  $A$ , взятое положительным, заведомо лежит между  $\sqrt{D} + B'$  и  $\sqrt{D} - B'$ . Если же  $A > \sqrt{D}$ , то не может быть  $B = 0$  (так как эти формы мы отбросили), а обязательно  $B = \frac{1}{2}A$ ; поэтому  $B'$  по величине равно  $\frac{1}{2}A$ , но имеет положительный знак (действительно, так как  $A < 2\sqrt{D}$ , то  $\pm \frac{1}{2}A$  лежит в границах, указанных для  $B'$ , и сравнимо с  $B$  по модулю  $A$ , а потому  $B' = \pm \frac{1}{2}A$ ), и тем самым  $B' < \sqrt{D}$ , т. е.  $2B' < \sqrt{D} + B'$  или  $A < \sqrt{D} + B'$ ; поэтому  $\pm A$  будет обязательно лежать между границами  $\sqrt{D} + B'$  и  $\sqrt{D} - B'$ . Наконец,  $W'$  содержит все приведенные собственно примитивные двусторонние формы с определителем  $D$ ; действительно, если  $(a, b, c)$  есть такая форма, то или  $b \equiv 0$  или  $b \equiv \frac{1}{2}a \pmod{a}$ . В первом случае, очевидно, не может быть  $b < a$ , а потому также и  $a > \sqrt{D}$ , вследствие чего форма  $(a, 0, -\frac{D}{a})$  заведомо содержится в  $W$ , а соответствующая форма  $(a, b, c)$  — в  $W'$ . Во втором случае



заведомо  $a < 2\sqrt{D}$  и потому  $\left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{a}\right)$  содержится в  $W$ , а соответствующая форма  $(a, b, c)$  — в  $W'$ . Из этого мы заключаем, что число форм в  $W$  равно числу всех приведенных собственно примитивных двусторонних форм с определителем  $D$ ; так как, однако, в каждом отдельном двустороннем классе содержатся две приведенные двусторонние формы (пп. 187, 194), то число всех двусторонних собственно примитивных классов с определителем  $D$  равно половине числа форм в  $W$ , т. е. половине всех возможных характеров.

## 259

*Число двусторонних несобственно примитивных классов с заданным определителем  $D$  всегда равно числу собственно примитивных двусторонних классов с тем же определителем.* Пусть  $K$  главный класс и  $K', K'', \dots$  — остальные двусторонние собственно примитивные классы того же определителя, далее,  $L$  — какой-нибудь двусторонний несобственно примитивный класс с этим же определителем, например, тот, в котором содержится форма  $\left(2, 1, \frac{1}{2} - \frac{1}{2}D\right)$ . Таким образом, при композиции класса  $L$  с  $K$  получается сам класс  $L$ ; при композиции же класса  $L$  с  $K', K'', \dots$  пусть получаются классы  $L', L'', \dots$ , которые, очевидно, все принадлежат тому же определителю, несобственно примитивны и двусторонни. Поэтому наша теорема будет доказана, если показать, что все классы  $L, L', L'', \dots$  различны, и что, кроме них, других несобственно примитивных двусторонних классов с определителем  $D$  нет. Для этой цели мы рассмотрим следующие случаи.

I. Если число несобственно примитивных классов равно числу собственно примитивных, то каждый из первых получается при композиции класса  $L$  с определенным собственно примитивным классом, вследствие чего все  $L, L', L'', \dots$  обязательно различны. Но если  $\mathfrak{L}$  обозначает какой-нибудь несобственно примитивный двусторонний класс с определителем  $D$ , то существует собственно примитивный класс  $\mathfrak{K}$  с тем свойством, что  $\mathfrak{K} + L = \mathfrak{L}$ ; если классу  $\mathfrak{K}$  противоположен класс  $\mathfrak{K}'$ , то будет также и  $\mathfrak{K}' + L = \mathfrak{L}$  (так как классы  $L, \mathfrak{L}$  противоположны самим себе), вследствие чего  $\mathfrak{K}$  и  $\mathfrak{K}'$  обязательно совпадают, и потому класс  $\mathfrak{K}$  является двусторонним.

Поэтому  $\mathfrak{K}$  находится среди классов  $K, K', K'', \dots$ , и  $\mathfrak{Q}$ —среди классов  $L, L', L'', \dots$ .

II. Если число несобственно примитивных классов втрое меньше, чем число собственно примитивных классов, то пусть  $H$ —класс, в котором содержится форма  $\left(4, 1, \frac{1-D}{4}\right)$ ,  $H'$ —класс, в котором содержится форма  $\left(4, 3, \frac{9-D}{4}\right)$ . Тогда  $H, H'$  собственно примитивны и отличны как один от другого, так и от главного класса  $K$ ; далее,  $H + H' = K$ ,  $2H = H'$ ,  $2H' = H$ , и если  $\mathfrak{Q}$ —какой-нибудь несобственно примитивный класс с определителем  $D$ , получающийся при композиции класса  $L$  с собственно примитивным классом  $\mathfrak{K}$ , то будет также  $\mathfrak{Q} = L + \mathfrak{K} + H$  и  $\mathfrak{Q} = L + \mathfrak{K} + H'$ ; кроме трех собственно примитивных и различных между собой классов  $\mathfrak{K}, \mathfrak{K} + H, \mathfrak{K} + H'$ , других классов, которые при композиции с  $L$  давали бы  $\mathfrak{Q}$ , не будет. А так как, если класс  $\mathfrak{Q}$  двусторонний, и  $\mathfrak{K}'$  противоположен классу  $\mathfrak{K}$ , также и  $L + K' = \mathfrak{Q}$ , то класс  $\mathfrak{K}'$  обязательно будет совпадать с одним из указанных трех классов. Если  $\mathfrak{K}' = \mathfrak{K}$ , то класс  $\mathfrak{K}$  двусторонний; если  $\mathfrak{K}' = \mathfrak{K} + H$ , то будет  $K = \mathfrak{K} + \mathfrak{K}' = 2\mathfrak{K} + H = 2(\mathfrak{K} + H')$ , и потому двусторонним будет  $\mathfrak{K} + H'$ , и аналогично, если  $\mathfrak{K}' = \mathfrak{K} + H'$ , то будет двусторонним  $\mathfrak{K} + H$ , откуда следует, что  $\mathfrak{Q}$  обязательно содержится среди классов  $L, L', L'', \dots$ . Но легко видеть, что среди трех классов  $\mathfrak{K}, \mathfrak{K} + H, \mathfrak{K} + H'$  больше чем одного двустороннего быть не может; действительно, если бы  $\mathfrak{K}$  и  $\mathfrak{K} + H$  оба были двусторонними, т. е. совпадали бы соответственно с противоположными им классами  $\mathfrak{K}', \mathfrak{K}' + H'$ , то было бы  $\mathfrak{K} + H = \mathfrak{K} + H'$ ; то же заключение получается из предположения, что двусторонни  $\mathfrak{K}$  и  $\mathfrak{K} + H'$ ; наконец, если бы  $\mathfrak{K} + H, \mathfrak{K} + H'$  были двусторонними, т. е. совпадали бы с противоположными им классами  $\mathfrak{K}' + H', \mathfrak{K}' + H$ , то было бы  $\mathfrak{K} + H + \mathfrak{K}' + H = \mathfrak{K}' + H' + \mathfrak{K} + H'$ , т. е.  $2H = 2H'$  или  $H = H'$ . Поэтому имеется только один двусторонний собственно примитивный класс, который при композиции с  $L$  дает  $\mathfrak{Q}$ , и, следовательно, все  $L, L', L'', \dots$  различны.

Число двусторонних классов в *произведенном* порядке, очевидно, равно числу двусторонних классов в *примитивном* порядке, из которого он произведен, и всегда может быть определено в силу предыдущего.

**Задача.** Собственно примитивный класс  $K$  с определителем  $D$  получается удвоением собственно примитивного класса  $k$  с тем же определителем; найти все такие классы, при удвоении которых получается класс  $K$ .

**Решение.** Пусть  $H$  главный класс определителя  $D$ , и  $H'$ ,  $H''$ ,  $H'''$ , ... — остальные двусторонние собственно примитивные классы с тем же определителем; обозначим классы, которые получаются при их композиции с  $k$ , именно,  $k + H'$ ,  $k + H''$ ,  $k + H'''$ , ... соответственно через  $k'$ ,  $k''$ ,  $k'''$ , ... Тогда все  $k$ ,  $k'$ ,  $k''$ , ... будут собственно примитивными классами с определителем  $D$ , различными между собой; точно так же легко видеть, что при удвоении этих отдельных классов получается класс  $K$ . Если же  $\mathfrak{K}$  обозначает какой-нибудь собственно примитивный класс с определителем  $D$ , который при удвоении дает класс  $K$ , то  $\mathfrak{K}$  обязательно будет содержаться среди классов  $k$ ,  $k'$ ,  $k''$ , ... Действительно, если положить  $\mathfrak{K} = k + \mathfrak{H}$ , так что  $\mathfrak{H}$  — собственно примитивный класс с определителем  $D$  (п. 249), то  $2k + 2\mathfrak{H} = 2\mathfrak{K} = K = 2k$ , откуда легко получается, что  $2\mathfrak{H}$  совпадает с главным классом,  $\mathfrak{H}$  — двусторонний класс, т. е. содержится среди классов  $H$ ,  $H'$ ,  $H''$ , ..., и  $\mathfrak{K}$  содержится среди классов  $k$ ,  $k'$ ,  $k''$ , ... Следовательно, эти классы будут представлять полное решение задачи.

Впрочем, ясно, что в случае, когда  $D$  отрицательно, среди классов  $k$ ,  $k'$ ,  $k''$ , ... половина положительных и половина отрицательных.

Так как тем самым каждый собственно примитивный класс с определителем  $D$ , который может быть получен удвоением подобного же класса, вообще получается при удвоении стольких подобных классов, сколько имеется двусторонних собственно примитивных классов с определителем  $D$ , то ясно, что если число всех собственно примитивных классов с определителем  $D$  равно  $r$ , а число всех двусторонних собственно примитивных классов с тем же определителем равно  $n$ , то число всех собственно примитивных классов с этим определителем, которые могут быть получены удвоением подобных классов, будет равно  $r/n$ . Та же формула получается, если в случае отрицательного определителя буквы  $r$ ,  $n$  обозначают количества положи-

*тельных* классов, именно, первая — количество *всех* собственно примитивных классов, а вторая — количество двусторонних собственно примитивных классов. Так, например, для определителя  $D = -161$  число всех положительных собственно примитивных классов равно 16, а число таких же двусторонних классов равно 4, и потому число всех классов, которые получаются удвоением подобных классов, должно быть равно 4. И действительно, мы находим, что все классы, содержащиеся в главном роде, обладают этим свойством; именно, главный класс  $(1, 0, 161)$  получается при удвоении четырех двусторонних классов;  $(2, 1, 81)$  — при удвоении классов  $(9, 1, 18)$ ,  $(9, -1, 18)$ ,  $(11, 2, 15)$ ,  $(11, -2, 15)$ ;  $(9, 1, 18)$  — при удвоении классов  $(3, 1, 54)$ ;  $(6, 1, 27)$ ,  $(5, -2, 33)$ ,  $(10, 3, 17)$ ; наконец,  $(9, -1, 18)$  — при удвоении классов  $(3, -1, 54)$ ,  $(6, -1, 27)$ ,  $(5, 2, 33)$ ,  $(10, -3, 17)$ .

**Половине всех возможных для данного определителя характеров заведомо не могут соответствовать собственно примитивные (при отрицательном определителе положительные) роды**

261

**Теорема.** *Половине всех возможных характеров не могут соответствовать при положительном определителе, не являющемся квадратом, собственно примитивные, а при отрицательном определителе собственно примитивные положительные роды.*

**Доказательство.** Пусть  $t$  — число всех собственно примитивных (положительных) родов определителя  $D$ ;  $k$  — число классов, содержащихся в отдельных родах, так что  $kt$  есть число всех собственно примитивных (положительных) классов, и  $n$  — число всех различных возможных для этого определителя характеров. Тогда, согласно п. 258, число всех двусторонних (положительных) собственно примитивных классов равно  $n/2$ , и потому, в соответствии с предыдущим пунктом, число всех собственно примитивных классов, которые могут получаться при удвоении подобных же классов, равно  $2kt/n$ . Но, согласно п. 247, все эти классы принадлежат главному роду, в котором содержится  $k$  классов. Если поэтому все

классы главного рода могут быть получены удвоением некоторых классов (в дальнейшем будет доказано, что в действительности это так и есть), то  $\frac{2km}{n} = k$  или  $m = \frac{1}{2}n$ ; но очевидно, что не может быть  $\frac{2km}{n} > k$ , и потому не может быть  $m > \frac{1}{2}n$ . Так как, следовательно, число всех собственно примитивных (положительных) родов заведомо не больше, чем половина всех возможных характеров, то по меньшей мере половине из них такие роды соответствовать не могут.

Впрочем, нужно отметить, что отсюда еще не следует, что половине всех возможных характеров действительно соответствуют собственно примитивные (положительные) роды; справедливость этой в высшей степени важной теоремы будет получена ниже из очень скрытых свойств чисел.

Так как для отрицательного определителя всегда существует столько же отрицательных родов, сколько и положительных, то очевидно, что из всех возможных характеров собственно примитивным отрицательным родам может принадлежать не более половины, о чем, так же, как и о несобственно примитивных родах, мы будем говорить ниже. Наконец, заметим, что теорема не распространяется на положительные квадратные определители, и что, напротив, для них отдельным возможным характерам действительно соответствуют роды.

### Второе доказательство фундаментальной теоремы и остальных теорем, касающихся вычетов $-1$ , $+2$ , $-2$

#### 262

Таким образом, в случае, когда для данного определителя  $D$ , не являющегося квадратом, возможны только два характера, собственно примитивный род будет соответствовать только одному из них (который обязательно является главным характером), в то время как другой не соответствует никакой собственно примитивной положительной форме этого определителя. Это имеет место для определителей  $-1$ ,  $2$ ,  $-2$ ,  $-4$ , для взятых положительными простыми числами вида  $4n + 1$ ,

для взятых отрицательными простыми чисел вида  $4n + 3$ , наконец, для всех взятых положительными нечетных степеней простых чисел вида  $4n + 1$  и для степеней простых чисел вида  $4n + 3$ , причем взятых положительными или отрицательными в зависимости от того, являются ли показатели четными или нечетными. На основании этого мы можем получить новый метод для того, чтобы доказать не только фундаментальную теорему, но и все остальные теоремы предыдущего раздела, касающиеся вычетов  $-1$ ,  $+2$ ,  $-2$ ,  $-$  метод, который совершенно отличен от использованного в предыдущем разделе и по изяществу ему не уступает. При этом, однако, мы отбросим определитель  $-4$  и определители, являющиеся степенями простых чисел, так как рассмотрение их не дает ничего нового.

Итак, для определителя  $-1$  не существует положительных форм, характером которых является  $3, 4$ ; для определителя  $+2$  вообще нет форм с характером  $3$  и  $5, 8$ ; для определителя  $-2$  нет положительных форм характера  $5$  и  $7, 8$ ; для определителя  $+p$ , если  $p$  — простое число вида  $4n + 1$ , или для определителя  $-p$ , если  $p$  — простое число вида  $4n + 3$ , не имеется собственно примитивных (в последнем случае положительных) форм характера  $Np$ . На основании этого мы докажем теоремы предыдущего раздела следующим образом.

I.— $-1$  является невычетом каждого (положительного) числа вида  $4n + 3$ . Действительно, если бы  $-1$  было вычетом некоторого такого числа  $A$ , то если положить  $-1 = B^2 - AC$ , форма  $(A, B, C)$  была бы положительной формой с определителем  $-1$ , характером которой было бы  $3, 4$ .

II.— $-1$  является вычетом каждого простого числа  $p$  вида  $4n + 1$ . Действительно, характером формы  $(-1, 0, p)$ , равно как и всех собственно примитивных форм с определителем  $p$ , является  $Rp$ ; поэтому  $-1$  есть вычет по модулю  $p$ .

III. Как  $+2$ , так и  $-2$  являются вычетами каждого простого числа  $p$  вида  $8n + 1$ . Действительно, формы  $\left(8, 1, \frac{1-p}{8}\right)$ ,  $\left(-8, 1, \frac{p-1}{8}\right)$  или формы  $\left(8, 3, \frac{9-p}{8}\right)$ ,  $\left(-8, 3, \frac{p-9}{8}\right)$  собственно примитивны (в зависимости от того, четно  $n$  или нечетно), и потому их

характер есть  $Rp$ . Следовательно,  $+8Rp$  и  $-8Rp$ , а потому также и  $2Rp$ ,  $-2Rp$ .

IV.  $+2$  является невычетом каждого числа вида  $8n + 3$  или  $8n + 5$ . Действительно, если бы  $+2$  было вычетом некоторого такого числа  $A$ , то существовала бы форма  $(A, B, C)$  с определителем  $+2$  с характером 3 и 5, 8.

V. Точно также  $-2$  является невычетом каждого числа вида  $8n + 5$  или  $8n + 7$ , так как иначе существовала бы форма с определителем  $-2$ , характером которой было бы 5 и 7, 8.

VI.  $-2$  является вычетом каждого простого числа  $p$  вида  $8n + 3$ . Эту теорему можно доказать двумя способами. Во-первых, так как, согласно IV,  $2Nr$  и, согласно I,  $-1Nr$ , то обязательно  $-2Rp$ . Второе доказательство основывается на рассмотрении определителя  $+2p$ , для которого возможно четыре характера, именно  $Rp$ , 1 и 3, 8;  $Rp$ , 5 и 7, 8;  $Np$ , 1 и 3, 8;  $Np$ , 5 и 7, 8, и из них по меньшей мере двум не соответствуют никакие роды. Но форме  $(1, 0, 2p)$  соответствует первый характер, а форме  $(-1, 0, 2p)$  — четвертый, поэтому должны быть отброшены второй и третий характеры. Так как характер формы  $(p, 0, -2)$  по отношению к числу 8 есть 1 и 3, 8, то ее характер по отношению к числу  $p$  не может быть иным, как  $Rp$ , и потому  $-2Rp$ .

VII.  $+2$  является вычетом каждого простого числа  $p$  вида  $8n + 7$ , что также можно доказать двумя способами. Во-первых, так как, согласно I и V,  $-1Nr$ ,  $-2Nr$ , то будет  $+2Rp$ . Во-вторых, так как или  $(8, 1, \frac{1+p}{8})$ , или  $(8, 3, \frac{9+p}{8})$  является собственно примитивной формой с определителем  $-p$  (в зависимости от того, четно  $n$  или нечетно), то ее характер есть  $Rp$ , и потому  $8Rp$  и  $2Rp$ .

VIII. Любое простое число  $p$  вида  $4n + 1$  является невычетом каждого нечетного числа  $q$ , которое есть невычет по модулю  $p$ . Действительно, если бы  $p$  было вычетом по модулю  $q$ , то, очевидно, имелась бы собственно примитивная форма с определителем  $p$ , характером которой было бы  $Np$ .

IX. Точно так же, если какое-нибудь нечетное число  $q$  является невычетом простого числа  $p$  вида  $4n + 3$ , то  $-p$  есть невычет по модулю  $q$ ; действительно, иначе имелась бы положительная собст-

венно примитивная форма с определителем  $-p$ , имеющая характер  $Np$ .

X. Каждое простое число  $p$  вида  $4n + 1$  является вычетом каждого другого простого числа  $q$ , которое есть вычет первого. Если  $q$  также имеет вид  $4n + 1$ , то это непосредственно следует из VIII; если же  $q$  имеет вид  $4n + 3$ , то (вследствие II) также и  $-q$  будет вычетом по модулю  $p$ , и потому  $pRq$  (согласно IX).

XI. Если какое-нибудь простое число  $q$  есть вычет другого простого числа  $p$  вида  $4n + 3$ , то  $-p$  является вычетом числа  $q$ . Именно, если  $q$  имеет вид  $4n + 1$ , то из VIII следует  $pRq$  и потому, согласно II,  $-pRq$ ; случай же, когда  $q$  имеет вид  $4n + 3$ , не поддается этому методу, но может быть легко изучен посредством рассмотрения определителя  $+pq$ . Именно, так как двум из четырех возможных для этого определителя характерам  $Rp, Rq; Rp, Nq; Np, Rq; Np, Nq$  не могут соответствовать роды, а характерами форм  $(1, 0, -pq)$ ,  $(-1, 0, pq)$  соответственно являются первый и четвертый, то второму и третьему характерам не может соответствовать никакая собственно примитивная форма с определителем  $pq$ . Так как теперь, по условию, характер формы  $(q, 0, -p)$  по отношению к числу  $p$  есть  $Rp$ , то характер этой формы по отношению к числу  $q$  должен быть  $Rq$ , и потому  $-pRq$ .

Если в теоремах VIII и IX предположить, что  $q$  обозначает простое число, то они в соединении с теоремами X и XI дадут фундаментальную теорему предыдущего раздела.

**Точнее определяется та половина характеров,  
которой не могут соответствовать роды**

После того, как мы заново доказали фундаментальную теорему, мы покажем, как та половина характеров, которой не могут соответствовать никакие собственно примитивные (положительные) формы, может быть определена для данного не являющегося квадратом определителя, причем мы решим эту задачу тем более просто, что фундамент для решения уже заложен в исследовании пп. 147—150. Пусть



$e^2$  есть наибольший квадрат, входящий в заданный определитель  $D$ , и  $D = D'e^2$ , так что  $D'$  не содержит квадратных множителей; далее, пусть  $a, b, c, \dots$  — все нечетные простые делители  $D'$ , и потому  $D'$ , с точностью до знака, есть или произведение этих чисел, или удвоенное произведение. Обозначим далее через  $\Omega$  совокупность специальных характеров  $Na, Nb, Nc, \dots$ , причем — только их, если  $D' \equiv 1 \pmod{4}$ ; с добавлением еще характера 3, 4, если  $D' \equiv 3$  и  $e$  или нечетно, или четно, но не делится на 4; с добавлением характеров 3, 8 и 7, 8, если  $D' \equiv 3$  и  $e$  делится на 4; с добавлением или характера 3 и 5, 8, или двух характеров 3, 8 и 5, 8, если  $D' \equiv 2 \pmod{8}$  и  $e$  или нечетно, или четно; наконец, с добавлением или характера 5 и 7, 8, или двух характеров 5, 8 и 7, 8, если  $D' \equiv 6 \pmod{8}$ , и  $e$  или нечетно, или четно. Если это сделано указанным образом, то все полные характеры, в которых содержится нечетное число специальных характеров из  $\Omega$ , не могут соответствовать никаким собственно примитивным (положительным) родам с определителем  $D$ . Во всех остальных случаях специальные характеры, которые выражают отношение к не входящим в  $D'$  простым делителям числа  $D$ , не имеют влияния на возможность или невозможность существования соответствующего рода. Из комбинаторных же соображений легко убедиться, что таким способом исключается действительно половина всех возможных полных характеров.

Доказательство справедливости этого правила проводится следующим образом. Из принципов предыдущего раздела или из заново доказанных в предыдущем пункте теорем без труда выводится, что если  $p$  есть какое-нибудь не входящее в  $D$  (нечетное положительное) простое число, которому отвечает какой-нибудь из отброшенных характеров, то  $D'$  содержит нечетное число сомножителей, являющихся невычетами по модулю  $p$ , а потому  $D'$ , а, значит, и  $D$ , есть невычет по модулю  $p$ . Далее, легко видеть, что произведение любого количества нечетных, взаимно простых с  $D$  чисел, которым не отвечает ни один из отброшенных характеров, также не может быть связано с таким характером; из этого, наоборот, ясно, что каждое нечетное положительное взаимно простое с  $D$  число, которое принадлежит какому-нибудь из отброшенных характеров, заведомо содержит какой-нибудь простой сомножитель с таким же свой-

ством, и потому  $D$  является его невычетом. Если бы поэтому существовала собственно примитивная (положительная) форма с определителем  $D$ , которая соответствует одному из отброшенных характеров, то  $D$  было бы невычетом каждого представимого такой формой положительного нечетного взаимно простого с  $D$  числа, что, очевидно, не согласуется с теоремой п. 154.

В качестве примеров можно сравнить классификации, указанные в пп. 231, 232, число которых при желании можно увеличить.

## 264

Итак, все возможные для какого-нибудь данного не являющегося квадратом определителя характеры разбиваются на два типа  $P$ ,  $Q$ , с тем свойством, что ни одному из характеров  $Q$  не может соответствовать собственно примитивная (положительная) форма, в то время как ничто, насколько мы до сих пор знаем, не препятствует тому, что остальным характерам  $P$  такие формы принадлежат. Относительно этого типа характеров можно, в частности, высказать следующую теорему, которая легко вытекает из их определения: если характер из  $P$  компонируется с характером из  $Q$  (по способу п. 246, т. е. точно так же, как если бы второму типу тоже соответствовал род), то получается характер из  $Q$ ; наоборот, если компонируются два характера из  $P$  или два характера из  $Q$ , то получающийся характер принадлежит к  $P$ . При помощи этой теоремы можно также и для отрицательных или несобственно примитивных родов исключить половину возможных характеров следующим образом.

I. Для отрицательного определителя  $D$  отрицательные роды будут в этом отношении как раз противоположны положительным, именно, ни один из характеров  $P$  не будет принадлежать собственно примитивному отрицательному роду, а все такие роды будут иметь характеры из  $Q$ . Действительно, если  $D' \equiv 1 \pmod{4}$ , то  $-D'$  является положительным числом вида  $4n + 3$ , и потому среди чисел  $a, b, c, \dots$  имеется нечетное количество чисел вида  $4n + 3$ , по каждому из которых  $-1$  есть невычет, откуда вытекает, что в полный характер формы  $(-1, 0, D)$  в этом случае входит нечетное число специальных характеров из  $\Omega$ , т. е. что он принадлежит  $Q$ . Если

$D' \equiv 3 \pmod{4}$ , то среди чисел  $a, b, c, \dots$  или совсем нет чисел вида  $4n + 3$ , или их имеется два, или четыре и т. д.; но так как в этом случае среди специальных характеров формы  $(-1, 0, D)$  встречается или 3, 4, или 3, 8, или 7, 8, то ясно, что и здесь полный характер этой формы принадлежит к  $Q$ . Тот же вывод так же легко получается и в остальных случаях, так что отрицательная форма  $(-1, 0, D)$  всегда имеет характер из  $Q$ . Но так как эта форма при композиции с какой-нибудь другой отрицательной собственно примитивной формой с тем же определителем дает положительную форму такого же типа, то легко видеть, что никакая отрицательная собственно примитивная форма не может иметь характера из  $P$ .

II. Для несобственно примитивных (положительных) родов подобным же образом доказывается, что дело обстоит или так же, как для собственно примитивных, или противоположным образом, в зависимости от того,  $D \equiv 1$  или  $\equiv 5 \pmod{8}$ . Действительно, в первом случае также и  $D' \equiv 1 \pmod{8}$ , откуда легко следует, что среди чисел  $a, b, c, \dots$  или совсем нет чисел вида  $8n + 3$  и  $8n + 5$ , или таковых имеется два, или четыре и т. д. (действительно, произведение любого количества нечетных чисел, среди которых чисел вида  $8n + 3$  и  $8n + 5$  вместе имеется нечетное количество, всегда будет или  $\equiv 3$ , или  $\equiv 5 \pmod{8}$ ), а произведение всех чисел  $a, b, c, \dots$  должно быть равно  $D'$  или  $-D'$ ). Отсюда вытекает, что полный характер формы  $(2, 1, \frac{1-D}{2})$  или не содержит специальных характеров из  $\Omega$ , или содержит их два, четыре и т. д., и потому принадлежит к  $P$ . Так как теперь каждая несобственно примитивная (положительная) форма с определителем  $D$  может рассматриваться как составленная из  $(2, 1, \frac{1-D}{2})$  и собственно примитивной (положительной) формы того же определителя, то ясно, что в этом случае никакая несобственно примитивная (положительная) форма не может иметь характера из  $Q$ . Во втором случае, когда  $D \equiv 5 \pmod{8}$ , все обстоит наоборот; именно, определитель  $D'$ , который тоже  $\equiv 5 \pmod{8}$ , заведомо содержит нечетное число сомножителей вида  $8n + 3$  и  $8n + 5$ , откуда следует, что характер формы  $(2, 1, \frac{1-D}{2})$ , а потому и характер каждой несобственно примитивной (положительной) формы с опре-

делителем  $D$  принадлежит к  $Q$ , т. е. никакому из характеров  $P$  не может соответствовать несобственно примитивный положительный род.

III. Наконец, для отрицательного определителя отрицательные несобственно примитивные роды снова противоположны несобственно примитивным положительным родам; именно, первые не могут иметь характеров из  $P$  или из  $Q$ , в зависимости от того,  $D \equiv 1$  или  $\equiv 5 \pmod{8}$ , или в зависимости от того, имеет ли  $-D$  вид  $8n + 7$  или  $8n + 3$ . Это без труда выводится из того, что при композиции формы  $(-1, 0, D)$ , характер которой принадлежит  $Q$ , с отрицательными несобственно примитивными формами того же определителя получаются положительные несобственно примитивные формы, и потому, если для последних исключены характеры  $Q$ , для первых обязательно должны быть исключены характеры  $P$ , и наоборот.

### Специальный метод для разложения простых чисел на два квадрата

265

Из исследований пп. 257, 258 относительно числа двусторонних классов, на которых базировалось все предыдущее, можно вывести еще много замечательных следствий, которые мы ради краткости опускаем; однако мы не можем пройти мимо следующего замечания, ввиду его изящества. Мы показали, что для положительного определителя  $p$ , являющегося простым числом вида  $4n + 1$ , имеется только один единственный двусторонний собственно примитивный класс; поэтому все двусторонние собственно примитивные формы с таким определителем собственно эквивалентны между собой. Следовательно, если  $b$  есть наибольшее положительное целое число, которое меньше чем  $\sqrt{p}$  и  $p - b^2 = a'$ , то формы  $(1, b, -a')$ .  $(-1, b, a')$  будут собственно эквивалентны, и потому, так как обе они, очевидно, являются приведенными, одна из них будет содержаться в периоде другой. Если первую форму снабдить в ее периоде индексом 0, то индекс второй обязательно будет нечетным (так как первые члены этих двух форм имеют противоположные знаки);

поэтому можно положить его равным  $2m + 1$ . Далее, легко видеть, что если формы с индексами  $1, 2, 3, \dots$  суть соответственно

$$(-a', b', a''), (a'', b'', -a'''), (-a''', b''', a'''), \dots,$$

то индексам  $2m, 2m - 1, 2m - 2, 2m - 3, \dots$  будут соответствовать формы

$$(a', b, -1), (-a'', b', a'), (a''', b'', -a''), (-a''', b''', a'''), \dots$$

Отсюда следует, что если форма индекса  $m$  равна  $(A, B, C)$ , то она же равна и  $(-C, B, -A)$ , и потому  $C = -A$  и  $p = A^2 + B^2$ . Поэтому каждое простое число вида  $4n + 1$  может быть разложено на два квадрата (данное разложение выше, в п. 182, мы вывели совсем из других принципов), и такое разложение мы получаем совсем простым и единообразным методом, именно, построением периода приведенной формы, определитель которой равен этому простому числу, а первый член равен 1, до формы, крайние члены которой равны по величине и противоположны по знаку. Так, например, для  $p = 233$  мы получаем следующий ряд форм:  $(1, 15, -8)$ ,  $(-8, 9, 19)$ ,  $(19, 10, -7)$ ,  $(-7, 11, 16)$ ,  $(16, 5, -13)$ ,  $(-13, 8, 13)$ , и  $233 = 64 + 169$ . Между прочим, ясно, что  $A$  обязательно нечетно (так как  $(A, B, -A)$  должна ведь быть собственно примитивной формой), и потому  $B$  будет четно. Так как для положительного определителя  $p$ , являющегося простым числом вида  $4n + 1$ , также и в несобственно примитивном порядке содержится только один единственный двусторонний класс, то очевидно, что если  $g$  есть наибольшее нечетное число, которое меньше чем  $\sqrt{p}$ , и  $p - g^2 = 4h$ , то приведенные несобственно примитивные формы  $(2, g, -2h)$ ,  $(-2, g, 2h)$  собственно эквивалентны, и потому одна из них содержится в периоде другой. Отсюда с помощью рассуждения, которое совершенно аналогично предыдущему, получается, что в периоде формы  $(2, g, -2h)$  находится форма, у которой крайние члены равны по величине, но противоположны по знаку, так что разложение числа  $p$  на два квадрата может быть выведено также и отсюда. Но очевидно, что крайние члены этой формы будут четными, а средний нечетным, и так как известно, что простое число может быть разложено на два квадрата только одним способом, то найденная этим

последним методом форма будет или  $(B, \pm A, -B)$ , или  $(-B, \pm A, B)$ . Так, в нашем примере для  $p = 233$  получается следующее:  $(2, 15, -4)$ ,  $(-4, 13, 16)$ ,  $(16, 3, -14)$ ,  $(-14, 11, 8)$ ,  $(8, 13, -8)$ , и  $233 = 64 + 169$ , как и выше.

### Отступление, содержащее исследование о тройничных формах

266

До сих пор мы ограничивали наше исследование такими функциями второй степени, которые содержат две переменные, и потому не было необходимости снабжать их специальным названием. Но очевидно, что мы можем рассматривать этот предмет как очень специальный раздел общего исследования *об алгебраических рациональных целых однородных функциях любого числа переменных и любой степени*, и подразделять такие функции *по степени на формы второй, третьей, четвертой и т. д. степеней*, и *по числу переменных на двойничные, тройничные, четверичные и т. д. формы*. Поэтому то, что до сих пор называлось просто формами, являются двойничными формами второй степени, а функции вида

$$Ax^2 + 2Bxy + Cy^2 + 2Dxz + 2Eyz + Fz^2$$

(где  $A, B, C, D, E, F$  обозначают заданные целые числа) — называются тройничными формами второй степени и т. д. Сначала настоящий раздел посвящался только двойничным формам второй степени; но так как остается еще много относящихся сюда фактов, причем из наиболее красивых, непосредственный источник которых следует искать в теории тройничных форм второй степени, мы хотим включить здесь краткое отступление об этой теории, в котором из первых ее элементов мы приведем то, что необходимо для пополнения теории двойничных форм, и надеемся, что для математиков это будет приятнее, чем если бы мы указанные факты или опустили, или вывели бы менее естественными методами. Более же подробное исследование об этом очень важном вопросе мы должны отложить до другого случая, во-первых, потому, что богатство его уже сейчас

очень расширило бы границы этого труда, а, во-вторых, потому, что имеется надежда на то, что в будущем оно пополнится еще другими важными фактами. Формы второй степени от четырех, пяти и т. д. переменных мы, по крайней мере в этом месте, совершенно исключаем из рассмотрения \*, и довольствуемся тем, что обращаем на эту весьма обширную область внимание математиков, ибо они найдут здесь обширный материал для упражнения своих сил и обогащения высшей арифметики выдающимися открытиями.

## 267

Для большей отчетливости будет очень полезно, если для трех входящих в тройничную форму переменных, как и в случае двойничных форм, мы установим определенный порядок расположения, так что первая, вторая и третья переменные будут различаться между собой. При размещении отдельных частей формы мы будем всегда соблюдать такой порядок, чтобы часть, содержащая квадрат первой переменной, занимала первое место, а далее следовали бы одна за другой части, содержащие квадрат второй переменной, квадрат третьей переменной, удвоенное произведение второй и третьей, удвоенное произведение первой и третьей, удвоенное произведение первой и второй переменной. Наконец, постоянные целые числа, на которые умножаются эти квадраты и удвоенные произведения, мы будем в том же порядке называть *первым, вторым, третьим, четвертым, пятым, шестым коэффициентами*.

Так, например,

$$ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

будет правильно расположенной тройничной формой, первая переменная которой есть  $x$ , вторая  $x'$ , третья  $x''$ , первый коэффициент которой есть  $a$ , и т. д., четвертый  $b$  и т. д. Так как, однако, в смысле краткости было бы удобно, если бы нам не нужно было бы всегда обозначать переменные тройничной формы специальными буквами, то мы будем записывать такую форму, если мы не

---

\* По этой же причине в дальнейшем под двойничными или тройничными формами все время будут пониматься формы *второй степени*.

обращаем внимания на переменные, следующим образом:

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}.$$

Если положить

$$\begin{aligned} b^2 - a'a'' &= A, & b'^2 - aa'' &= A', & b''^2 - aa' &= A'', \\ ab - b'b'' &= B, & a'b' - bb'' &= B', & a''b'' - bb' &= B'', \end{aligned}$$

то получается *другая форма*

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} = F,$$

которую мы будем называть *дополнительной к форме*

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} = f.$$

Отсюда, если для краткости положить

$$ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2bb'b'' = D,$$

мы снова находим

$$\begin{aligned} B^2 - A'A'' &= aD, & B'^2 - AA'' &= a'D, & B''^2 - AA' &= a''D, \\ AB - B'B'' &= bD, & A'B' - BB'' &= b'D, & A''B'' - BB' &= b''D, \end{aligned}$$

откуда вытекает, что дополнительной для формы  $F$  является форма

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}.$$

Число  $D$ , от свойств которого в первую очередь зависят свойства тройничной формы  $f$ , мы будем называть *определителем этой формы*. Таким образом, определитель формы  $F$  будет равен  $D^2$ , т. е. равен квадрату определителя формы  $f$ , для которой она является дополнительной.

Так, например, для тройничной формы

$$\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix}$$



дополнительной будет форма

$$\begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & -133 \end{pmatrix}$$

и определитель обеих равен 1.

Тройничные формы с определителем 0 мы из последующего исследования совершенно исключим, так как они, как будет показано в оставленной до другого случая более полной теории тройничных форм, только по виду являются тройничными формами, в действительности же эквивалентны двойничным формам.

## 268

Если какая-нибудь тройничная форма  $f$  с определителем  $D$ , переменными которой являются  $x, x', x''$  (именно, первая равна  $x$ , и т. д.), переходит в тройничную форму  $g$  с определителем  $E$ , переменными которой являются  $y, y', y''$ , при подстановке вида

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'', \\ x' &= \alpha' y + \beta' y' + \gamma' y'', \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'', \end{aligned}$$

где все девять коэффициентов  $\alpha, \beta, \dots$  предполагаются целыми числами, то мы, ради краткости, будем, отбрасывая переменные, говорить просто, что  $f$  переходит в  $g$  при подстановке  $(S)$

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{array}$$

и что  $f$  содержит форму  $g$  или  $g$  содержится в  $f$ . Из этого предположения непосредственно получается, следовательно, шесть равенств для шести коэффициентов формы  $g$ , приводить которые здесь нет нужды; однако из них несложными выкладками получаются следующие выводы.

I. Если положить для краткости

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'' = k,$$

то после соответствующих сокращений получается равенство  $E = k^2 D$ , откуда вытекает, что  $E$  делится на  $D$  и отношение является квадратом. Поэтому ясно, что число  $k$  является для преобразований тройничных форм подобным числу  $\alpha\delta - \beta\gamma$  из п. 157 для преобразований двойничных форм, именно, квадратным корнем из отношения определителей, из чего можно было бы предположить, что различие знаков у  $k$  и здесь обуславливает существенное различие между преобразованиями и собственной и несобственной содержимостью одной формы в другой. Однако, если рассмотреть вопрос ближе, то видно, что  $f$  переходит в  $g$  также и при подстановке

$$\begin{array}{lll} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma'', \end{array}$$

но если в значение  $k$  подставить  $-\alpha$  вместо  $\alpha$ ,  $-\beta$  вместо  $\beta$ , и т. д. то получится  $-k$ , и потому эта подстановка будет неоднотипна с подстановкой  $(S)$ , а, значит, каждая тройничная форма, которая содержит другую форму каким-нибудь образом, содержит ее и другим образом. Поэтому такое различие здесь делаться не будет, так как для тройничных форм оно не нужно.

II. Если обозначить через  $F, G$  формы, дополнительные к  $f, g$ , то коэффициенты у  $F$  будут определяться коэффициентами формы  $f$ , а коэффициенты у  $G$  — значениями коэффициентов формы  $g$ , которые известны из равенств, определяемых подстановкой  $S$ .

Если выразить коэффициенты формы  $f$  буквами, то сравнением значений коэффициентов форм  $F, G$  без труда устанавливается, что  $F$  содержит форму  $G$  и переходит в нее при подстановке  $(S')$

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\beta'' - \alpha''\beta', \\ \beta\gamma - \beta\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\beta - \alpha\beta'', \\ \beta\gamma' - \beta'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\beta' - \alpha'\beta. \end{array}$$

Выкладку, которая не требует преодоления никаких трудностей, мы здесь не выписываем.

III. При подстановке  $(S'')$

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \beta''\gamma - \beta\gamma'', & \beta\gamma' - \beta'\gamma, \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha, \\ \alpha'\beta'' - \alpha''\beta', & \alpha''\beta - \alpha\beta'', & \alpha\beta' - \alpha'\beta \end{array}$$

форма  $g$  переходит, очевидно, в ту форму, в которую переходит форма  $f$  при подстановке

$$\begin{aligned} k, 0, 0 \\ 0, k, 0 \\ 0, 0, k, \end{aligned}$$

т. е. она переходит в ту форму, которая получается, если отдельные коэффициенты формы  $f$  умножить на  $k^2$ . Эту форму мы обозначим через  $f'$ .

IV. Точно таким же образом показывается, что  $G$  при подстановке  $(S''')$

$$\begin{aligned} \alpha, \alpha', \alpha'' \\ \beta, \beta', \beta'' \\ \gamma, \gamma', \gamma'' \end{aligned}$$

переходит в форму, которая получается из  $F$ , если отдельные коэффициенты у  $F$  умножить на  $k^2$ . Эту форму мы обозначим через  $F'$ .

Мы будем говорить, что подстановка  $S'''$  получается из подстановки  $S$  *транспонированием*; тогда  $S$ , очевидно, тоже будет получаться транспонированием из подстановки  $S'''$ , и из подстановок  $S'$ ,  $S''$  одна будет получаться транспонированием другой. Подстановку  $S'$  целесообразно назвать дополнительной к подстановке  $S$ , и потому  $S''$  будет также дополнительной к подстановке  $S'''$ .

Если не только форма  $f$  содержит форму  $g$ , но и вторая форма содержит первую, то формы  $f$ ,  $g$  называются *эквивалентными*. В этом случае не только  $D$  входит в  $E$ , но и  $E$  входит в  $D$ , откуда легко следует, что  $D = E$ . Но и наоборот, если форма  $f$  содержит форму  $g$  с тем же определителем, то обе эти формы эквивалентны. Действительно (если использовать те же обозначения, что и в предыдущем пункте, и исключить случай  $D = 0$ ),  $k = \pm 1$ , и потому форма  $f'$ , в которую переходит  $g$  при подстановке  $S''$ , идентична  $f$ , т. е.  $f$  содержится в  $g$ . Далее, ясно, что в этом случае также и дополнительные к  $f$ ,  $g$  формы  $F$ ,  $G$  эквивалентны между собой, и вторая

переходит в первую при подстановке  $S'''$ . Наконец, если, наоборот, *предполагать* формы  $F, G$  эквивалентными, причем считать, что первая переходит во вторую при подстановке  $T$ , то и формы  $f, g$  будут эквивалентны, и  $f$  будет переходить в  $g$  при подстановке, дополнительной к  $T$ , а  $g$  в  $f$  при подстановке, которая получается из  $T$  транспонированием. Действительно, при этих двух подстановках соответственно форма, дополнительная к  $F$ , переходит в форму, дополнительную к  $G$ , и вторая в первую; но обе эти формы получаются из  $f, g$  умножением отдельных коэффициентов на  $D$ , откуда без труда следует, что при указанных выше подстановках соответственно  $f$  переходит в  $g$ , и  $g$  в  $f$ .

## 270

Если тройничная форма  $f$  содержит тройничную форму  $f'$ , а последняя, в свою очередь, содержит форму  $f''$ , то и  $f$  будет содержать форму  $f''$ . Действительно, легко видеть, что если переходят

| $f$ в $f'$ при подстановке    | $f'$ в $f''$ при подстановке         |
|-------------------------------|--------------------------------------|
| $\alpha, \beta, \gamma$       | $\delta, \varepsilon, \zeta$         |
| $\alpha', \beta', \gamma'$    | $\delta', \varepsilon', \zeta'$      |
| $\alpha'', \beta'', \gamma''$ | $\delta'', \varepsilon'', \zeta''$ , |

то  $f$  будет преобразовываться в  $f''$  при подстановке

$$\begin{aligned} &\alpha\delta + \beta\delta' + \gamma\delta'', & \alpha\varepsilon + \beta\varepsilon' + \gamma\varepsilon'', & \alpha\zeta + \beta\zeta' + \gamma\zeta'', \\ &\alpha'\delta + \beta'\delta' + \gamma'\delta'', & \alpha'\varepsilon + \beta'\varepsilon' + \gamma'\varepsilon'', & \alpha'\zeta + \beta'\zeta' + \gamma'\zeta'', \\ &\alpha''\delta + \beta''\delta' + \gamma''\delta'', & \alpha''\varepsilon + \beta''\varepsilon' + \gamma''\varepsilon'', & \alpha''\zeta + \beta''\zeta' + \gamma''\zeta''. \end{aligned}$$

Таким образом, если  $f$  эквивалентна форме  $f'$ , и  $f'$  эквивалентна форме  $f''$ , то форма  $f$  также будет эквивалентна форме  $f''$ . Ясно, как эти теоремы распространяются на большее число форм.

## 271

Отсюда уже вытекает, что *все тройничные формы*, так же, как и двойничные, *могут быть разбиты на классы*, если причислять эквивалентные формы к одному и тому же классу, а не эквивалент-

ные — к различным. Формы с различными определителями будут поэтому заведомо принадлежать к различным классам, и потому будет бесконечно много классов тройничных форм; принадлежащие же одному и тому же определителю тройничные формы образуют или большее, или меньшее число классов; но как *основное свойство* этих форм следует рассматривать то, что все формы с одним и тем же заданным определителем всегда образуют конечное число классов. Подробному изложению этой очень важной теоремы мы должны предпослать установление следующего важного различия, которое имеет место для тройничных форм.

Некоторые тройничные формы устроены так, что ими могут представляться как положительные, так и отрицательные числа, например, форма  $x^2 + y^2 - z^2$ ; вследствие этого они называются **неопределенными формами**. Напротив, другими формами не могут представляться отрицательные числа, а только положительные (кроме нуля, который получается, если все переменные положить равными 0), например, формой  $x^2 + y^2 + z^2$ ; вследствие этого такие формы называются **положительными**; наконец, некоторыми формами не могут представляться положительные числа, например, формой  $-x^2 - y^2 - z^2$ , вследствие чего они называются **отрицательными формами**. Положительные и отрицательные формы имеют общее название: **определенные формы**. Сейчас мы уже дадим некоторые критерии, при помощи которых можно судить об этих свойствах форм.

Если тройничную форму

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

с определителем  $D$  умножить на  $a$  и так же, как в п. 267, обозначить коэффициенты дополнительной к  $f$  формы через  $A, A', A'', B, B', B''$ , то получается форма

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = g;$$

если теперь еще раз умножить на  $A'$ , то получим форму

$$A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'^2 = h.$$

Из этого тотчас же вытекает, что если как  $A'$ , так и  $aD$  являются отрицательными числами, то все значения  $h$  отрицательны, вследствие чего формой  $f$ , очевидно, могут представляться только такие числа, знаки которых противоположны знаку  $aA'$ , т. е. совпадают со знаком  $a$  или противоположны знаку  $D$ . Таким образом, в этом случае  $f$  является определенной формой, причем положительной или отрицательной в зависимости от того, положительно  $a$  или отрицательно, или в зависимости от того, отрицательно  $D$  или положительно.

Если же или оба числа  $aD$ ,  $A'$  положительны, или одно положительно, а другое отрицательно (ни одно не равно 0), то легко видеть, что  $h$  при соответствующем определении величин  $x$ ,  $x'$ ,  $x''$  может принимать как положительные, так и отрицательные значения. Следовательно, в этом случае  $f$  может принимать значения, которые имеют или тот же знак, что и  $aA'$ , или противоположный, и потому  $f$  будет неопределенной формой.

В случае, когда  $A' = 0$ , но  $a$  не равно 0, должно быть

$$g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2bx'').$$

Если придать  $x'$  произвольное значение (которое, однако, не равно 0 и выбрать  $x''$  так, чтобы  $\frac{A''x'}{2B} - x''$  имело тот же знак, что и  $Bx'$  (легко видеть, что это возможно, так как  $B$  не может быть равно нулю; действительно, в противном случае было бы  $B^2 - A'A'' = aD = 0$ , и потому  $D = 0$ , а этот случай мы исключили), то  $x'(A''x' - 2Bx'')$  будет положительной величиной, откуда легко вытекает, что  $x$  можно определить так, чтобы  $g$  получило отрицательное значение. Очевидно, что при желании эти значения можно подобрать и так, чтобы все они были целыми числами. Наконец, ясно, что если  $x'$ ,  $x''$  приданы любые значения, то  $x$  можно взять столь большим, что  $g$  будет положительно. Поэтому  $f$  является в этом случае неопределенной формой.

Наконец, если  $a = 0$ , то

$$f = a'x'^2 + 2bx'x'' + a''x''^2 + 2x(b''x' + b'x'').$$

Поэтому если взять  $x'$ ,  $x''$  произвольными, но такими, что  $b''x' + b'x''$  не равно 0 (что, очевидно, возможно, если только  $b'$  и  $b''$  не

равны одновременно 0; но тогда было бы  $D = 0$ ), то легко видеть, что  $x$  можно определить так, чтобы  $f$  принимала как положительные, так и отрицательные значения. Следовательно, и в этом случае  $f$  есть неопределенная форма.

Тем же способом, каким мы здесь по числам  $aD$ ,  $A'$  определяли природу формы  $f$ , можно делать это и при помощи чисел  $aD$  и  $A''$ , так что  $f$  является определенной формой, если как  $aD$ , так и  $A''$  отрицательны, и неопределенной во всех остальных случаях. И точно так же этой цели может служить рассмотрение чисел  $a'D$  и  $A$ , или чисел  $a'D$  и  $A''$ , или чисел  $a''D$  и  $A$ , или, наконец, чисел  $a''D$  и  $A'$ .

Из всего этого следует, что у определенной формы шесть чисел  $A$ ,  $A'$ ,  $A''$ ,  $aD$ ,  $a'D$ ,  $a''D$  отрицательны, причем у положительной формы  $a$ ,  $a'$ ,  $a''$  положительны,  $D$  отрицательно, а у отрицательной формы  $a$ ,  $a'$ ,  $a''$  отрицательны и  $D$  положительно. Отсюда вытекает, что все тройничные формы с заданным положительным определителем распадаются на отрицательные и неопределенные формы, все тройничные формы с заданным отрицательным определителем распадаются на положительные и неопределенные, и, наконец, что положительных форм с положительным определителем или отрицательных с отрицательным определителем вообще не существует. Кроме того, легко видеть, что для определенной формы дополнительной всегда является определенная и притом отрицательная форма, а для неопределенной — неопределенная.

Так как все числа, представляемые данной тройничной формой, очевидно, представляются также и всеми эквивалентными ей формами, то содержащиеся в одном и том же классе тройничные формы будут или все неопределенными, или все положительными, или все отрицательными. Поэтому эти наименования можно перенести с форм на целые классы.

Высказанную в предыдущем пункте теорему о том, что все тройничные формы с заданным определителем распадаются на *конечное* число классов, мы докажем методом, подобным тому, который мы

использовали для двойничных форм, именно, мы покажем, *во-первых*, каким образом каждая тройничная форма может быть сведена к более простой форме, и, *во-вторых*, что количество простейших форм (к которым мы приходим при этой редукции) для каждого данного определителя конечно. Если мы вообще предположим, что дана тройничная форма  $f = \begin{pmatrix} a, a', a'' \\ b, b', b'' \end{pmatrix}$  с (отличным от нуля) определителем  $D$ , которая при подстановке

$$(S) \quad \begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta' & \gamma' \\ \alpha'' & \beta'', & \gamma'' \end{array}$$

переходит в эквивалентную форму  $g = \begin{pmatrix} m, m', m'' \\ n, n', n'' \end{pmatrix}$ , то наша задача состоит в том, чтобы определить  $\alpha, \beta, \gamma, \dots$ , так, чтобы форма  $g$  была проще чем  $f$ . Если дополнительными для форм  $f, g$  являются соответственно формы  $\begin{pmatrix} A, A', A'' \\ B, B', B'' \end{pmatrix}, \begin{pmatrix} M, M', M'' \\ N, N', N'' \end{pmatrix}$ , которые мы обозначим через  $F, G$ , то, согласно п. 269,  $F$  переходит в  $G$  при подстановке, дополнительной к  $S$ , а  $G$  в  $F$  при подстановке, получающейся из  $S$  транспонированием. Число

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma'',$$

которое должно быть равно или  $+1$ , или  $-1$ , мы обозначим через  $k$ . После этого заметим следующее.

I. Если  $\gamma = 0, \gamma' = 0, \alpha'' = 0, \beta'' = 0, \gamma'' = 1$ , то

$$\begin{aligned} m &= a\alpha^2 + 2b''\alpha\alpha' + a'\alpha'^2, & m' &= a\beta^2 + 2b''\beta\beta' + a'\beta'^2, & m'' &= a''; \\ n &= b\beta' + b'\beta, & n' &= b\alpha' + b'\alpha, & n'' &= a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta'. \end{aligned}$$

Кроме того,  $\alpha\beta' - \beta\alpha'$  должно быть равно или  $+1$ , или  $-1$ . Из этого вытекает, что двойничная форма  $(a, b'', a')$ , определитель которой есть  $A''$ , при подстановке  $\alpha, \beta, \alpha', \beta'$  преобразуется в двойничную форму  $(m, n'', m')$  с определителем  $M''$ , и потому, вследствие  $\alpha\beta' - \beta\alpha' = \pm 1$ , ей эквивалентна, откуда следует  $M'' = A''$ , что легко может быть установлено и непосредственно. Если поэтому  $(a, b'', a')$



сама еще не является простейшей формой в своем классе, то  $\alpha, \beta, \alpha', \beta'$  могут быть определены так, что  $(m, n'', m')$  будет более простой формой, причем из теории эквивалентности двойничных форм легко следует, что это может быть сделано так, что  $m$  не больше чем  $\sqrt{-4A''/3}$ , если  $A''$  отрицательно, или не больше чем  $\sqrt{A''}$ , если  $A''$  положительно, или  $m = 0$ , если  $A'' = 0$ , так что во всех случаях (абсолютная) величина  $m$  заведомо может считаться или равной 0, или по крайней мере не превосходящей  $\sqrt{\pm 4A''/3}$ . Итак, при этом форма  $f$  сводится к другой форме, которая, если это вообще возможно, имеет меньший первый коэффициент, а дополнительная к ней форма имеет такой же третий коэффициент, что и дополнительная к  $f$  форма  $F$ . В этом состоит первая редукция.

II. Если, напротив,  $\alpha = 1, \beta = 0, \gamma = 0, \alpha' = 0, \alpha'' = 0$ , то  $k' = \beta'\gamma'' - \beta''\gamma' = \pm 1$ ; поэтому подстановкой, дополнительной к  $S$ , является

$$\begin{array}{ccc} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta', \end{array}$$

и посредством нее  $F$  переводится в  $G$ . Мы имеем поэтому

$$\begin{aligned} m &= a, \quad n' = b'\gamma'' + b''\gamma', & n'' &= b'\beta'' + b''\beta', \\ m' &= \alpha'\beta'^2 + 2b\beta'\beta'' + a''\beta''^2, & m'' &= a'\gamma'^2 + 2b\gamma'\gamma'' + a''\gamma''^2, \\ n &= a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'', \\ M' &= A'\gamma''^2 - 2B\gamma'\gamma'' + A''\gamma'^2, \\ N &= -A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma', \\ M'' &= A'\beta''^2 - 2B\beta'\beta'' + A''\beta'^2. \end{aligned}$$

Отсюда вытекает, что двойничная форма  $(A'', B, A')$ , определитель которой есть  $Da$ , при подстановке  $\beta', -\gamma', -\beta'', \gamma''$  переходит в форму  $(M'', N, M')$  с определителем  $Dm$ , и потому (вследствие того, что  $\beta'\gamma'' - \gamma'\beta'' = \pm 1$ , или того, что  $Da = Dm$ ) эквивалентна ей. Если поэтому  $(A'', B, A')$  еще не является простейшей формой своего класса, то коэффициенты  $\beta', \gamma', \beta'', \gamma''$  могут быть определены так, что форма  $(M'', N, M')$  будет более простой, причем это всегда может быть достигнуто так, что  $M''$ , рассматриваемое без знака, не больше чем  $\sqrt{\pm 4Da/3}$ . Следовательно, таким способом фор-

ма  $f$  сводится к другой форме с таким же первым коэффициентом, а форма, дополнительная к этой второй форме, имеет третий коэффициент, который, если это вообще возможно, меньше, чем третий коэффициент дополнительной к  $f$  формы  $F$ . В этом состоит **вторая редукция**.

III. Если поэтому  $f$  есть тройничная форма, к которой не применима ни первая, ни вторая редукция, т. е. которая ни одной из этих двух редукций не может быть сведена к более простой форме, то по абсолютной величине обязательно будет как  $a^2 \leq \frac{4}{3}A''$ , так и  $A''^2 \leq \frac{4}{3}aD$ . Из этого следует, что  $a^4 \leq \frac{16}{9}A''^2$ , и потому  $a^4 \leq \frac{64}{27}aD$  или  $a^3 \leq \frac{64}{27}D$  и  $a \leq \frac{4}{3}\sqrt[3]{D}$ ; отсюда снова  $A''^2 \leq \frac{16}{9}\sqrt[3]{D^4}$  и  $A'' \leq \frac{4}{3}\sqrt[3]{D^2}$ . Поэтому если  $a$  или  $A''$  еще превосходят эти границы, то к форме  $f$  обязательно будет применима одна из предыдущих редукций. Впрочем, это утверждение нельзя обратить, так как часто бывает, что тройничная форма, у которой ее первый коэффициент и третий коэффициент дополнительной формы уже лежат в указанных границах, все же может быть сделана еще проще при помощи первой или второй редукции.

IV. Если теперь к любой заданной тройничной форме с определителем  $D$  попеременно применять первую и вторую редукции, т. е. если к ней самой применить первую, к получающейся при этом форме вторую или первую, к так полученной форме снова первую или вторую редукцию и т. д., то ясно, что в конце концов мы придем к форме, к которой уже не применима ни одна из этих редукций. Действительно, так как абсолютные величины как первых коэффициентов получающихся при этом форм, так и третьих коэффициентов дополнительных к ним форм попеременно то остаются неизменными, то убывают, этот процесс обязательно будет где-нибудь иметь конец, ибо иначе получились бы два бесконечных ряда постоянно убывающих чисел. Из этого мы уже получаем следующую красивую теорему. *Каждая тройничная форма с определителем  $D$  может быть сведена к другой эквивалентной ей форме, у которой*

первый коэффициент не больше чем  $\frac{4}{3}\sqrt[3]{D}$ , а третий коэффициент дополнительной к ней формы не больше чем  $\frac{4}{3}\sqrt[3]{D^2}$  (по абсолютной величине), если сама заданная форма еще не обладает этими свойствами. Впрочем, если бы вместо первого коэффициента формы  $f$  и третьего коэффициента дополнительной к ней формы мы точно таким же образом взяли бы или первый коэффициент самой формы и второй коэффициент дополнительной, или второй коэффициент самой формы и первый или третий коэффициент дополнительной, или третий коэффициент самой формы и первый или второй коэффициент дополнительной, мы тем же самым путем достигли бы своей цели; однако целесообразно все время придерживаться одного метода, чтобы иметь возможность легче производить относящиеся сюда операции по определенному алгоритму. Заметим, наконец, что для обоих коэффициентов, для которых мы показали, как можно заключить их в определенные границы, могут быть установлены еще меньшие границы, если отделить определенные формы от неопределенных; однако для нашей теперешней цели это не нужно.

## 273

Теперь мы дадим несколько примеров, на которых указанные перед этим правила сделаются яснее.

**Пример 1.** Если

$$f = \begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix},$$

то

$$F = \begin{pmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{pmatrix}$$

и  $D = -1$ . Так как  $(19, 1, 21)$  является приведенной двойничной формой, которой никакая другая форма с меньшим первым членом, чем 19, не эквивалентна, то первая редукция здесь не применима; напротив, мы находим, что двойничная форма  $(-398, 257, -166)$ ,

согласно теории эквивалентности двойничных форм, преобразуема в более простую эквивалентную ей форму  $(-2, 1, -10)$ , причем первая переходит во вторую при подстановке  $2, 7, 3, 11$ .

Поэтому если положить  $\beta' = 2$ ,  $\gamma' = -7$ ,  $\beta'' = -3$ ,  $\gamma'' = 11$ , то к форме  $f$  применяется подстановка

$$\begin{array}{ccc} 1, & 0, & 0 \\ 0, & 2, & -7, \\ 0, & -3, & 11 \end{array}$$

при которой она переходит в форму

$$f = \begin{pmatrix} 19, 354, 4769 \\ -1299, 301, -82 \end{pmatrix}.$$

Третий коэффициент дополнительной к ней формы равен  $-2$ , и в этом отношении  $f'$  проще, чем  $f$ .

К форме  $f'$  можно применить первую редукцию. Именно, так как двойничная форма  $(19, -82, 354)$  переходит в форму  $(1, 0, 2)$  при подстановке  $13, 4, 3, 1$ , то к форме  $f'$  нужно применить подстановку

$$\begin{array}{ccc} 13, & 4, & 0 \\ 3, & 1, & 0, \\ 0, & 0, & 1 \end{array}$$

при которой она переходит в

$$f'' = \begin{pmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{pmatrix}.$$

К форме  $f''$ , дополнительной к которой является форма

$$\begin{pmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{pmatrix},$$

можно снова применить вторую редукцию. Именно, форма  $(-2, -95, -4513)$  при подстановке  $47, 1, -1, 0$  переходит в  $(-1, 1, -2)$ ; поэтому к форме  $f''$  нужно применить подстановку

$$\begin{array}{ccc} 1, & 0, & 0 \\ 0, & 47, & -1, \\ 0, & 1, & -1 \end{array}$$

при которой она переходит в

$$f''' = \begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}.$$

Первый коэффициент этой формы дальше уже первой подстановкой уменьшен быть не может, так же, как и третий коэффициент дополнительной к ней формы, — второй подстановкой.

**Пример 2.** Если дана форма

$$f = \begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix},$$

дополнительной к которой является форма

$$\begin{pmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{pmatrix}$$

и определитель которой равен 2, то, применяя в соответствии с правилами попеременно вторую и первую редукции, мы находим

| подстановки,                                                              | при которых<br>переходит | в                                                                    |
|---------------------------------------------------------------------------|--------------------------|----------------------------------------------------------------------|
| $\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{matrix}$ | $f$                      | $\begin{pmatrix} 10, & 2, & 2 \\ -1, & 0, & -4 \end{pmatrix} = f'$   |
| $\begin{matrix} 0, & -1, & 0 \\ 1, & -2, & 0 \\ 0, & 0, & 1 \end{matrix}$ | $f'$                     | $\begin{pmatrix} 2, & 2, & 2 \\ 2, & -1, & 0 \end{pmatrix} = f''$    |
| $\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 2, & -1 \end{matrix}$ | $f''$                    | $\begin{pmatrix} 2, & 2, & 2 \\ -2, & 1, & -2 \end{pmatrix} = f'''$  |
| $\begin{matrix} 1, & 0, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}$   | $f'''$                   | $\begin{pmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{pmatrix} = f''''$ |

Форма  $f'''$  не может быть дальше упрощена ни первой, ни второй редукцией.

Если имеется тройничная форма, у которой первый коэффициент, так же, как и третий коэффициент дополнительной к ней формы,

уменьшены при помощи только что указанных методов насколько это возможно, то дальнейшую редукцию дает следующий метод.

Если мы сохраним те же обозначения, что и в п. 272, и положим  $\alpha = 1$ ,  $\alpha' = 0$ ,  $\beta' = 1$ ,  $\alpha'' = 0$ ,  $\beta'' = 0$ ,  $\gamma'' = 1$ , т. е. сделаем подстановку

$$\begin{aligned} &1, \beta, \gamma \\ &0, 1, \gamma' \\ &0, 0, 1, \end{aligned}$$

то будет

$$\begin{aligned} m &= a, \quad m' = a' + 2b''\beta + a\beta^2, \\ m'' &= a'' + 2\beta\gamma' + 2b'\gamma + a\gamma^2 + 2b''\gamma\gamma' + a'\gamma'^2, \\ n &= b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma, \quad n' = b' + a\gamma + b''\gamma', \\ n'' &= b'' + a\beta; \end{aligned}$$

кроме того,

$$M'' = A'', \quad N = B - A''\gamma', \quad N' = B' - N\beta - A''\gamma.$$

Итак, при такой подстановке коэффициенты  $a$ ,  $A''$ , которые понижались предыдущими редукциями, не изменяются; поэтому наша задача состоит в том, чтобы посредством оответствующего выбора  $\beta$ ,  $\gamma$ ,  $\gamma'$  добиться уменьшения других коэффициентов. Для этой цели заметим сначала, что если  $A'' = 0$ , то можно считать, что и  $a = 0$ ; действительно, если бы  $a$  не было равно 0, то была бы еще раз применима первая редукция, так как каждая двойничная форма с определителем 0 эквивалентна форме вида  $(0, 0, h)$ , т. е. форме, первый член которой равен 0 (ср. п. 215). По совершенно аналогичной причине можно предполагать, что если  $a = 0$ , то и  $A'' = 0$ , так что или ни одно из чисел  $a$ ,  $A''$  не равно 0, или они равны 0 оба.

В первом случае ясно, что  $\beta$ ,  $\gamma$ ,  $\gamma'$  могут быть определены так, что по абсолютной величине  $n''$ ,  $N$ ,  $N'$  будут соответственно не больше чем  $\frac{1}{2}a$ ,  $\frac{1}{2}A''$ ,  $\frac{1}{2}A''$ . Так, в первом примере предыдущего пункта последняя форма

$$\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix},$$

дополнительной к которой является форма

$$\begin{pmatrix} -513, & -2, & -1 \\ & 1, & -16, & 32 \end{pmatrix},$$

при подстановке

$$\begin{pmatrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{pmatrix}$$

переходит в форму

$$\begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix} = f''',$$

дополнительной к которой будет форма

$$\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}.$$

Во втором случае, когда  $a = A'' = 0$  и потому также  $b'' = 0$ , будет

$$\begin{aligned} m &= 0, \quad m' = a', \quad m'' = -a'' + 2b\gamma' + 2b'\gamma + a'\gamma'^2; \\ n &= b + a'\gamma' + b'\beta, \quad n' = b', \quad n'' = 0. \end{aligned}$$

Поэтому

$$D = a'b'^2 = m'n'^2,$$

и легко видеть, что  $\beta$  и  $\gamma'$  могут быть определены так, что  $n$  будет равно абсолютно наименьшему вычету числа  $b$  по модулю, являющемуся наибольшим общим делителем  $a'$ ,  $b'$ , т. е. что по абсолютной величине будет не больше половины этого делителя, и потому  $n = 0$ , если  $a'$ ,  $b'$  взаимно просты. Если  $\beta$ ,  $\gamma'$  определены таким образом, то значение  $\gamma$  может быть выбрано так, что  $m''$  по абсолютной величине будет не больше чем  $b'$ ; это было бы невозможно сделать только в том случае, если  $b' = 0$ ; но тогда было бы  $D = 0$ , однако этот случай мы исключили. Так, для последней формы во втором примере предыдущего пункта  $n = -2 - \beta + 2\gamma'$ , откуда, если положить  $\beta = -2$ ,  $\gamma' = 0$ , следует  $n = 0$ , далее,  $m'' = 2 - 2\gamma$ , и, если положить  $\gamma = 1$ , то  $m'' = 0$ . Мы получаем поэтому подстановку

$$\begin{array}{ccc} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1, \end{array}$$

при которой указанная форма переходит в

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix} = f''''.$$

### 275

Если имеются ряд эквивалентных тройничных форм  $f, f', f'', f''', \dots$  и преобразования каждой из этих форм в следующую, то, в соответствии с п. 270, из преобразований  $f$  в  $f'$  и  $f'$  в  $f''$  выводится преобразование формы  $f$  в  $f''$ ; из него и из преобразования формы  $f''$  в  $f'''$  следует преобразование формы  $f$  в  $f'''$  и т. д., и очевидно, что таким способом можно найти преобразование формы  $f$  в любую форму ряда. А так как из преобразования формы  $f$  в какую-нибудь эквивалентную ей форму  $g$  может быть получено и преобразование формы  $g$  в  $f$  ( $S''$  из  $S$ , пп. 268, 269), то можно таким путем найти преобразование любой формы ряда  $f', f'', \dots$  в первую форму  $f$ . Так, для форм первого примера предыдущего пункта мы находим подстановки

$$\begin{array}{ccc|ccc} 13, & 4, & 0 & 13, & 188, & -4 \\ 6, & 2, & -7 & 6, & 87, & -2 \\ -9, & -3, & 11 & -9, & -130, & 3 \end{array} \quad \begin{array}{ccc} 13, & -20, & 16 \\ 6, & -9, & 7 \\ -9, & 14, & -11, \end{array}$$

которыми форма  $f$  переводится соответственно в  $f'', f''', f''''$ , а из последней подстановки находим следующую:

$$\begin{array}{ccc} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3, \end{array}$$

при которой  $f''''$  переходит в  $f$ . Подобным же образом во втором примере предыдущего пункта получаются подстановки

$$\begin{array}{ccc|ccc} 1, & -1, & 1 & 2, & -3, & -1 \\ -3, & 4, & -3 & 3, & 1, & 0 \\ 10, & -14, & 11 & 2, & 4, & 1, \end{array}$$



при которых соответственно форма

$$\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$$

переходит в

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix},$$

и вторая — в первую.

## 276

**Теорема.** Число классов, на которые распадаются все тройничные формы с данным определителем, всегда конечно.

**Доказательство.** I. Число всех форм  $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$  с данным определителем  $D$ , у которых  $a = 0$ ,  $b'' = 0$ ,  $b$  не больше, чем половина наибольшего общего делителя чисел  $a'$ ,  $b'$ , и  $a''$  не больше чем  $b'$ , очевидно, конечно. Действительно, так как должно быть  $a'b'^2 = D$ , для значения  $b'$  не имеется других возможностей, кроме  $+1$ ,  $-1$  и корней из входящих в  $D$  квадратов (если, кроме 1, еще имеются таковые) с положительными или отрицательными знаками, а количество этих значений конечно. Для отдельных же значений  $b'$  значения  $a'$  определены, а значения  $b$ ,  $a''$ , очевидно, ограничены конечным числом возможностей.

II. Точно так же количество всех форм  $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$  с определителем  $D$ , у которых  $a$  не равно 0 и не больше чем  $\frac{4}{3}\sqrt[3]{\pm D}$ ,  $b''^2 - aa' = A''$  не равно нулю и не больше чем  $\frac{4}{3}\sqrt[3]{D^2}$ ,  $b''$  не больше чем  $a/2$ ,  $ab - b'b'' = B$  и  $a'b' - bb'' = B'$  не больше чем  $\frac{1}{2}A''$ , конечно. Действительно, количество всех комбинаций значений  $a$ ,  $b''$ ,  $A''$ ,  $B$ ,  $B'$  конечно; если же эти значения заданы, то остальные коэффициенты формы  $a'$ ,  $b$ ,  $b'$ ,  $a''$  и коэффициенты

$$b^2 - a'a'' = A, \quad b'^2 - aa'' = A', \quad a''b'' - bb' = B''$$

дополнительной формы определяются из следующих равенств:

$$\begin{aligned} a' &= \frac{b''^2 - A''}{a}, & A' &= \frac{B^2 - aD}{A''}, & A &= \frac{B'^2 - a'D}{A''}, & B'' &= \frac{BB' + b''D}{A''}, \\ b &= \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, & b' &= \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}, \\ a'' &= \frac{b'^2 - A'}{a} = \frac{b^2 - A}{a'} = \frac{bb' + B''}{b''}. \end{aligned}$$

А так как указанные формы получаются, если из всех комбинаций значений  $a, b'', A'', B, B'$  выбрать те, для которых значения  $a', a'', b, b'$  получаются целыми, то количество этих форм, очевидно, конечно.

III. Итак, все формы из I и II вместе образуют конечное число классов, которое может быть и меньше, чем число форм, если какие-нибудь из них эквивалентны между собой. А так как, в силу предыдущих исследований, каждая тройничная форма с определителем  $D$  обязательно эквивалентна одной из этих форм, т. е. принадлежит какому-нибудь из классов, образуемых этими формами, то эти классы охватывают все формы с определителем  $D$ , т. е. все тройничные формы с определителем  $D$  распадаются на конечное число классов.

## 277

Правила, по которым могут быть найдены все формы в I и II предыдущего пункта, получаются сами собой из изложенного, вследствие чего можно ограничиться приведением нескольких примеров.

Для  $D = 1$  получаются следующие шесть (вследствие двойных знаков) форм I:

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 1 \end{pmatrix};$$

у форм II  $a$  и  $A''$  не могут иметь других значений, кроме  $+1$  и  $-1$ , а для получающихся из них четырех комбинаций  $b'', B$  и  $B'$  должны быть положены равными 0; таким образом, получаются четыре формы:

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}.$$

Точно так же для  $D = -1$  получается шесть форм I и четыре формы II, именно:

$$\begin{pmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & -1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \begin{pmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \\ \begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix},$$

Для  $D = 2$  получается шесть форм I:

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix},$$

и восемь форм II:

$$\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \\ \begin{pmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{pmatrix}.$$

Впрочем, число получающихся из этих форм в этих трех случаях классов много меньше, чем число форм. Именно, легко устанавливается следующее.

I. Форма

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$$

переходит в

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

соответственно при подстановках

$$\begin{array}{ccc|ccc|ccc} 1, & 0, & 0 & 0, & 0, & 1 & 0, & 0, & 1 & 1, & 0, & -1 \\ 0, & 1, & 0 & 0, & 1, & -1 & 0, & 1, & 1 & 1, & 1, & -1 \\ 0, & 0, & -1 & 1, & 1, & 0 & 1, & -1, & -1 & 0, & -1, & 1, \end{array}$$

а форма

$$\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

переходит в

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$$

простой перестановкой переменных. Поэтому десять указанных тройничных форм с определителем 1 сводятся к двум:

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix};$$

вместо первой при желании можно взять и следующую:

$$\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}.$$

Так как первая форма неопределенная, а вторая определенная, то ясно, что каждая неопределенная тройничная форма с определителем 1 эквивалентна форме  $x^2 + 2yz$ , а каждая определенная — форме  $-x^2 - y^2 - z^2$ .

II. Совершенно аналогично находим, что каждая неопределенная тройничная форма с определителем  $-1$  эквивалентна форме  $-x^2 + 2yz$ , а каждая определенная — форме  $x^2 + y^2 + z^2$ .

III. Для определителя 2 из восьми форм II сразу могут быть отброшены вторая, шестая и седьмая, так как они получаются из первой простой перестановкой переменных, и по такой же причине — пятая, которая получается из третьей подобным же образом, и восьмая, получающаяся из четвертой. Остальные три образуют вместе с шестью формами I три класса; именно,

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}$$

переходит в

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$$

при подстановке

$$\begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1, \end{pmatrix}$$

а форма

$$\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$$

переходит в формы

$$\begin{pmatrix} 0, & 2, & 1 \\ 0, & 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & 1 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & -1 \\ 0, & 1, & 0 \end{pmatrix}, \\ \begin{pmatrix} 0, & 2, & -1 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}$$

соответственно при подстановках

$$\begin{array}{c} 1, \ 0, \ 1 \mid 1, \ 0, \ -1 \mid 1, \ 0, \ 0 \mid 1, \ 0, \ 0 \mid 1, \ 0, \ 0 \\ 1, \ 2, \ 0 \mid 1, \ 2, \ 0 \mid 1, \ 2, \ -1 \mid 1, \ 2, \ 1 \mid 0, \ 1, \ 2 \\ 1, \ 1, \ 0 \mid 1, \ 1, \ 0 \mid 1, \ 1, \ -1 \mid 1, \ 1, \ 1 \mid 0, \ 1, \ 1. \end{array}$$

Поэтому каждая тройничная форма с определителем 2 приводится к какой-нибудь из следующих трех форм:

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix},$$

вместо первой из которых при желании можно взять также форму

$$\begin{pmatrix} 2, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}.$$

Но очевидно, что каждая определенная тройничная форма обязательно будет эквивалентна третьей форме, —  $x^2 - y^2 - 2z^2$ , так как первые две формы неопределенные, а каждая неопределенная форма будет эквивалентна первой или второй, а именно, первой,  $2x^2 + 2yz$ , если ее первый, второй и третий коэффициенты одновременно четны (так как легко видеть, что такая форма при любом преобразовании переходит в подобную же форму и потому не может быть эквивалентна второй форме), и второй,  $x^2 + y^2 - 2z^2$ , если ее первый,

второй и третий коэффициенты не являются одновременно четными, т. е. или один из них, или два, или все три нечетны (действительно, по аналогичной причине в такую форму форма  $2x^2 + 2yz$  не может перейти ни при какой подстановке).

Таким образом, то, что получилось в примерах пп. 273, 274, а именно, что определенная форма

$$\begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$$

с определителем  $-1$  приводится к форме  $x^2 + y^2 + z^2$ , а неопределенная форма

$$\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$$

с определителем  $2$  — к форме  $2x^2 - 2yz$  или (что сводится к тому же) к форме  $2x^2 + 2yz$ , можно было бы на основании приведенного исследования предсказать заранее.

## 278

*Тройничной формой с переменными  $x, x', x''$  представляются с одной стороны, числа, когда  $x, x', x''$  придаются определенные значения, а с другой стороны — двойничные формы, посредством подстановок вида*

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

где  $m, n, m', \dots$  обозначают определенные числа, а  $t, u$  — переменные представляемой формы. Для полноты теории тройничных форм было бы поэтому нужно решить следующие задачи.

I. Найти все представления заданного числа заданной тройничной формой.

II. Найти все представления заданной двойничной формы заданной тройничной формой.

III. Определить, эквивалентны ли две заданные тройничные формы с одинаковым определителем, или нет, и в первом случае найти все преобразования первой формы во вторую.

IV. Определить, содержит ли заданная тройничная форма другую заданную тройничную форму с бóльшим определителем, или нет, и в первом случае определить все преобразования первой формы во вторую.

На этих задачах, которые значительно труднее, чем аналогичные задачи для двойничных форм, мы подробно остановимся в другом месте; здесь мы ограничим наше исследование тем, что покажем, как первая задача может быть сведена ко второй, а вторая — к третьей; третью же мы научимся решать для нескольких простейших и для теории двойничных форм особенно важных случаев; четвертой задачи мы не будем рассматривать совсем.

## 279

*Лемма. Если даны три любых целых числа  $a, a', a''$  (которые, однако, не все одновременно равны нулю), то можно найти шесть других чисел  $B, B', B'', C, C', C''$  с тем свойством, что*

$$B'C'' - B''C' = a, \quad B''C - BC'' = a', \quad BC' - B'C = a''.$$

*Доказательство.* Пусть  $\alpha$  — наибольший общий делитель чисел  $a, a', a''$ ; возьмем такие целые числа  $A, A', A''$ , что

$$Aa + A'a' + A''a'' = \alpha.$$

Далее, возьмем три любых целых числа  $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$  с тем только условием, что три числа  $\mathfrak{C}'A'' - \mathfrak{C}''A'$ ,  $\mathfrak{C}''A - \mathfrak{C}A''$ ,  $\mathfrak{C}A' - \mathfrak{C}'A$ , которые мы соответственно обозначим через  $b, b', b''$ , а их наибольший общий делитель через  $\beta$ , не все одновременно равны нулю. Если положить тогда

$$a'b'' - a''b' = \alpha\beta C, \quad a''b - ab'' = \alpha\beta C', \quad ab' - a'b = \alpha\beta C'',$$

то числа  $C, C', C''$ , очевидно, будут целыми. Наконец, если мы выберем целые числа  $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$  так, что

$$\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta,$$

положим

$$\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = h,$$

и затем положим

$$B = \alpha \mathfrak{B} - hA, \quad B' = \alpha \mathfrak{B}' - hA', \quad B'' = \alpha \mathfrak{B}'' - hA'',$$

то эти значения  $B, B', B'', C, C', C''$  будут удовлетворять предписанным условиям.

Именно, мы находим

$$aB + a'B' + a''B'' = 0,$$

$$bA + b'A' + b''A'' = 0, \text{ и потому } bB + b'B' + b''B'' = \alpha\beta.$$

Теперь из значений  $C', C''$  мы получаем

$$\begin{aligned} \alpha\beta (B'C'' - B''C') &= ab'B' - a'bB' - a''bB'' + ab''B'' = \\ &= a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\beta a, \end{aligned}$$

и потому  $B'C'' - B''C' = a$ , и подобным же образом находим, что  $B''C - BC'' = a'$ ,  $BC' - B'C = a''$ .

В остальном анализ, при помощи которого это решение было найдено, а также метод для отыскания по одному решению всех других здесь должны быть опущены.

280

Предположим, что двойничная форма

$$at^2 + 2btu + cu^2 = \varphi,$$

определитель которой пусть равен  $D$ , представляется тройничной формой  $f$  от переменных  $x, x', x''$ , если положить

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

и что дополнительной к форме  $f$  является форма  $F$  от переменных  $X, X', X''$ . Тогда легко установить выкладкой (если обозначить коэффициенты форм  $f, F$  специальными буквами), а также сразу выводится из п. 268, II, что число  $D$  представляется формой  $F$ , если положить

$$X = m'n'' - m''n', \quad X' = m''n - mn'', \quad X'' = mn' - m'n;$$

это представление числа  $D$  естественно назвать дополнительным к представлению формы  $\varphi$  формой  $f$ . Если значения  $X, X', X''$



не имеют общих делителей, мы будем называть это представление числа  $D$  собственным, в противном же случае — несобственным, и будем применять те же наименования и в отношении представления формы  $\varphi$  формой  $f$ , к которому первое представление является дополнительным. Отыскание всех собственных представлений числа  $D$  формой  $F$  основывается на следующем.

I. Не существует представления числа  $D$  формой  $F$ , которое не могло бы быть выведено из некоторого представления какой-нибудь формы с определителем  $D$  формой  $f$ , т. е. не было бы дополнительным к такому представлению.

Именно, пусть представление числа  $D$  формой  $F$  следующее;  $X = L$ ,  $X' = L'$ ,  $X'' = L''$ ; возьмем на основании леммы предыдущего пункта, такие  $m$ ,  $m'$ ,  $m''$ ,  $n$ ,  $n'$ ,  $n''$ , что

$$m'n'' - m''n' = L, \quad m''n - mn'' = L', \quad mn' - m'n = L'',$$

и пусть  $f$  при подстановке

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

переходит в двойничную форму  $\varphi = at^2 + 2btu + cu^2$ . Тогда легко видеть, что  $D$  есть определитель формы  $\varphi$ , и заданное представление числа  $D$  формой  $F$  является дополнительным к представлению формы  $\varphi$  формой  $f$ .

**Пример.** Пусть  $f = x^2 + x'^2 + x''^2$ , и потому  $F = -X^2 - X'^2 - X''^2$ ,  $D = -209$ , и представление  $D$  формой  $F$  следующее:  $X=1$ ,  $X'=8$ ,  $X''=12$ . Отсюда для  $m$ ,  $m'$ ,  $m''$ ,  $n$ ,  $n'$ ,  $n''$  мы находим следующие значения:  $-20$ ,  $1$ ,  $1$ ,  $-12$ ,  $0$ ,  $1$ , и  $\varphi = 402t^2 + 482tu + 145u^2$ .

II. Если  $\varphi$ ,  $\chi$  — собственно эквивалентные двойничные формы, то каждое представление числа  $D$  формой  $F$ , являющееся дополнительным к некоторому представлению формы  $\varphi$  формой  $f$ , будет также дополнительным и к некоторому представлению формы  $\chi$  формой  $f$ .

Если переменные формы  $\chi$  суть  $p, q$ , при собственной подстановке  $t = \alpha p + \beta q$ ,  $u = \gamma p + \delta q$  форма  $\varphi$  переходит в  $\chi$ , и некоторым представлением формы  $\varphi$  формой  $f$  является

$$(R) \quad x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

то без труда видно, что если положить

$$\begin{aligned}\alpha m + \gamma n &= g, \quad \alpha m' + \gamma n' = g', \quad \alpha m'' + \gamma n'' = g'' \\ \beta m + \delta n &= h, \quad \beta m' + \delta n' = h', \quad \beta m'' + \delta n'' = h'',\end{aligned}$$

то форма  $\chi$  будет представляться формой  $f$  при

$$(R') \quad x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q,$$

и если произвести выкладки, то мы найдем (в силу  $\alpha\delta - \beta\gamma = 1$ ), что

$$\begin{aligned}g'h'' - g''h' &= m'n'' - m''n', \quad g''h - gh'' = m''n - mn'', \\ gh' - g'h &= mn' - m'n,\end{aligned}$$

т. е. это представление числа  $D$  формой  $F$  эквивалентно представлениям  $(R)$ ,  $(R')$ .

Так, мы находим, что в предыдущем примере форме  $\varphi$  эквивалентна форма  $\chi = 13p^2 - 10pq + 18q^2$ , причем первая переходит во вторую при собственной подстановке  $t = -3p + q$ ,  $u = 5p - 2q$ . Отсюда мы находим следующее представление формы  $\chi$  формой  $f$ :  $x = 4q$ ,  $x' = -3p + q$ ,  $x'' = 2p - q$ , из которого получается то же самое представление числа  $-209$ , из которого мы и исходили.

III. Наконец, если две двойничные формы  $\varphi$ ,  $\chi$  с определителем  $D$ , зависящие соответственно от переменных  $t, u$ ;  $p, q$ , представляются формой  $f$ , и для какого-нибудь представления одной из них дополнительным собственным представлением числа  $D$  формой  $F$  является то же представление, что и для некоторого представления другой, то эти формы обязательно собственно эквивалентны. Предположим, что форма  $\varphi$  представляется формой  $f$ , если положить

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

а форма  $\chi$  — если положить

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q,$$

и что

$$\begin{aligned}m'n'' - m''n' &= g'h'' - g''h' = L, \\ m''n - mn'' &= g''h - gh'' = L', \\ mn' - m'n &= gh' - g'h = L''.\end{aligned}$$

Подберем целые числа  $l, l', l''$  так, что  $Ll + L'l' + L''l'' = 1$ , и положим

$$\begin{aligned} n'l'' - n''l' &= M, \quad n''l - nl'' = M', \quad nl' - n'l = M'', \\ l'm'' - l''m' &= N, \quad l''m - lm'' = N', \quad lm' - l'm = N''. \end{aligned}$$

Наконец, положим

$$\begin{aligned} gM + g'M' + g''M'' &= \alpha, \quad hM + h'M' + h''M'' = \beta, \\ gN + g'N' + g''N'' &= \gamma, \quad hN + h'N' + h''N'' = \delta. \end{aligned}$$

Отсюда легко получить, что

$$\begin{aligned} \alpha m + \gamma n &= g - l(gL + g'L' + g''L'') = g, \\ \beta m + \delta n &= h - l(hL + h'L' + h''L'') = h, \end{aligned}$$

и точно так же

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''.$$

Из этого вытекает, что выражения  $mt + nu$ ,  $m't + n'u$ ,  $m''t + n''u$  при подстановке

$$(S) \quad t = \alpha p + \beta q, \quad u = \gamma p + \delta q$$

переходят соответственно в  $gp + hq$ ,  $g'p + h'q$ ,  $g''p + h''q$ , откуда явствует, что при подстановке (S) форма  $\varphi$  переходит в ту же форму, в которую переходит  $f$ , если положить

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q,$$

т. е. в форму  $\chi$ , которой она поэтому эквивалентна. Наконец, после соответствующих выкладок легко находится, что

$$\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1,$$

вследствие чего подстановка (S) является собственной, и формы  $\varphi$ ,  $\chi$  собственно эквивалентны.

Из этих замечаний вытекают следующие правила для отыскания всех собственных представлений числа  $D$  формой  $F$ . Нужно найти все классы двойничных форм с определителем  $D$  и из каждого класса выбрать произвольную форму; далее, нужно найти все собственные представления этих отдельных форм формой  $f$  (причем те формы, которые формой  $f$  не представляются, отбрасываются) и

из этих представлений вывести представления числа  $D$  формой  $F$ . Из I и II следует, что при этом будут получены все возможные собственные представления, и потому задача будет решена полностью; из III следует, что преобразования форм из различных классов заведомо приводят к различным представлениям.

## 281

Отыскание *несобственных* представлений заданного числа  $D$  формой  $F$  легко может быть сведено к предыдущему случаю. Именно, ясно, что если  $D$  не делится ни на какой квадрат (кроме 1), то таких представлений вообще нет, а в том случае, когда  $D$  делится на квадраты  $\lambda^2, \mu^2, \nu^2, \dots$ , все несобственные представления числа  $D$  формой  $F$  будут найдены, если найти все собственные представления этой формой чисел  $D/\lambda^2, D/\mu^2, D/\nu^2, \dots$  и умножить значения переменных соответственно на  $\lambda, \mu, \nu, \dots$ .

Итак, отыскание всех представлений заданного числа заданной тройничной формой, являющейся дополнительной к некоторой тройничной форме, свелось ко второй задаче; а к этому случаю, который на первый взгляд кажется очень частным, могут быть следующим образом сведены остальные случаи. Пусть  $D$  — число, которое нужно представить формой  $\begin{pmatrix} g & g' & g'' \\ h & h' & h'' \end{pmatrix}$ , определитель которой равен  $\Delta$ , и дополнительной к которой является форма  $\begin{pmatrix} G & G' & G'' \\ H & H' & H'' \end{pmatrix} = f$ . Последней форме снова эквивалентна форма  $\begin{pmatrix} \Delta g & \Delta g' & \Delta g'' \\ \Delta h & \Delta h' & \Delta h'' \end{pmatrix} = F$  и ясно, что представления формой  $F$  числа  $\Delta D$  (находить которые можно на основании предыдущего) полностью идентичны представлениям заданной формой числа  $D$ . Заметим, что если все коэффициенты формы  $f$  имеют общий делитель  $\mu$ , то все коэффициенты формы  $F$ , очевидно, делятся на  $\mu^2$ , вследствие чего и  $\Delta D$  должно делиться на  $\mu^2$  (иначе представлений не будет), и представления числа  $D$  заданной формой будут идентичны представлениям числа  $\Delta D/\mu^2$  той формой, которая получается

из  $F$ , если отдельные коэффициенты формы  $F$  умножить на  $\mu^2$ , и которая является дополнительной для формы, получающейся из формы  $f$ , если ее отдельные коэффициенты поделить на  $\mu$ .

Отметим, наконец, что это решение первой задачи неприменимо, если  $D = 0$ , так как в этом случае двойничные формы с определителем  $D$  разбиваются на бесконечное число классов; ниже мы разберем этот случай при помощи других принципов.

## 282

*Отыскание представлений заданной двойничной формы, определитель которой не равен нулю \**, заданной тройничной формой основывается на следующих замечаниях.

I. Из каждого собственного представления двойничной формы  $(p, q, r) = \varphi$  с определителем  $D$  тройничной формой  $f$  с определителем  $\Delta$  могут быть найдены целые числа  $B, B'$  с тем свойством, что

$$B^2 \equiv \Delta p, \quad BB' \equiv -\Delta q, \quad B'^2 \equiv \Delta r \pmod{D}.$$

или, другими словами, может быть получено значение выражения  $\sqrt{\Delta(p, -q, r)} \pmod{D}$ . Пусть мы имеем следующее собственное представление формы  $\varphi$  формой  $f$ :

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

(где  $x, x', x''; t, u$  обозначают соответственно переменные форм  $f; \varphi$ ); подберем целые числа  $\gamma, \gamma', \gamma''$  так, чтобы число

$$(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma'' = k$$

было равно или  $+1$ , или  $-1$ ; пусть при подстановке

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

---

\* Случай  $D = 0$ , который рассматривается при помощи совершенно других методов, здесь, ради краткости, опускается.

форма  $f$  переходит в форму  $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix} = g$ , дополнительной к которой является форма  $\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \end{pmatrix} = G$ . Тогда ясно, что  $a = p$ ,  $b'' = q$ ,  $a' = r$ ,  $A'' = D$ , и определителем формы  $g$  является  $\Delta$ . Поэтому

$$B^2 = \Delta p + A'D, \quad BB' = -\Delta q + B''D, \quad B'^2 = \Delta r + AD.$$

Так, например, форма  $19t^2 + 6tu + 41u^2$  будет представляться формой  $x^2 + x'^2 + x''^2$  при  $x = 3t + 5u$ ,  $x' = 3t - 4u$ ,  $x'' = t$ , откуда следует, что если положить  $\gamma = -1$ ,  $\gamma' = 1$ ,  $\gamma'' = 0$ , то  $B = -171$ ,  $B' = 27$ , т. е.  $(-171, 27)$  является значением выражения  $\sqrt{-1(19, -3, 41)} \pmod{770}$ .

Отсюда уже следует, что если  $\Delta(p, -q, r)$  не является квадратичным вычетом по модулю  $D$ , то форма  $\varphi$  не может быть собственно представлена никакой тройничной формой с определителем  $\Delta$ ; поэтому в случае, когда  $\Delta, D$  взаимно просты,  $\Delta$  должно быть характеристическим числом формы  $\varphi$ .

II. Так как числа  $\gamma, \gamma', \gamma''$  могут быть выбраны бесчисленным множеством способов, то могут получаться различные значения для  $B, B'$ , и мы хотим узнать, в какой связи они находятся между собой. Предположим, что и числа  $\delta, \delta', \delta''$  таковы, что

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$$

равно или  $+1$ , или  $-1$ , и что форма  $f$  при подстановке

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

переходит в форму  $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix} = g$ , дополнительной к которой является форма  $\begin{pmatrix} \mathfrak{A} & \mathfrak{A}' & \mathfrak{A}'' \\ \mathfrak{B} & \mathfrak{B}' & \mathfrak{B}'' \end{pmatrix} = \mathfrak{G}$ . Тогда формы  $g, \mathfrak{g}$  эквивалентны.

а поэтому эквивалентны также и формы  $G$ ,  $\mathfrak{G}$ , и применяя указанные в пп. 269, 270 принципы, мы находим\*, что если положить

$$\begin{aligned}(\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' &= \zeta, \\ (\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' &= \eta,\end{aligned}$$

то форма  $\mathfrak{G}$  будет переходить в  $G$  при подстановке

$$\begin{aligned}k, & 0, 0 \\ 0, & k, 0 \\ \zeta, & \eta, \mathfrak{k}.\end{aligned}$$

Следовательно,

$$B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}, \quad B' = \zeta\mathfrak{k}D + \mathfrak{k}kB',$$

и потому, в силу того, что  $\mathfrak{k}k = \pm 1$ , имеет место или  $B \equiv \mathfrak{B}$ ,  $B' \equiv \mathfrak{B}'$ , или  $B \equiv -\mathfrak{B}$ ,  $B' \equiv -\mathfrak{B}' \pmod{D}$ . В первом случае мы назовем значения  $(B, B')$ ,  $(\mathfrak{B}, \mathfrak{B}')$  эквивалентными, а во втором — противоположными; о представлении же формы  $\varphi$  мы будем говорить, что оно принадлежит некоторому значению выражения  $\sqrt{\Delta(p, -q, r)} \pmod{D}$ , которое может быть получено из этого представления методом, изложенным в I. Поэтому все значения, которым принадлежит одно и то же представление, будут или эквивалентны, или противоположны.

III. Наоборот, если, как и раньше в I, представление  $x = \alpha t + \beta u, \dots$  формы  $\varphi$  формой  $f$  принадлежит значению  $(B, B')$ , которое может быть выведено отсюда при помощи преобразования

$$\begin{aligned}\alpha, & \beta, \gamma \\ \alpha', & \beta', \gamma' \\ \alpha'', & \beta'', \gamma'',\end{aligned}$$

то это же представление будет принадлежать также и каждому другому значению  $(\mathfrak{B}, \mathfrak{B}')$ , которое либо эквивалентно, либо противоположно первому, т. е. вместо  $\gamma, \gamma', \gamma''$  можно брать другие целые

---

\* Именно, если из преобразования формы  $f$  в  $g$  вывести преобразование  $g$  в  $f$ , из этого последнего и из преобразования формы  $f$  в  $\mathfrak{g}$  вывести преобразование формы  $g$  в  $\mathfrak{g}$ , и, наконец, отсюда посредством транспонирования получить преобразование  $\mathfrak{G}$  в  $G$ .

числа  $\delta, \delta', \delta''$ , для которых выполняется следующее равенство:

$$(\Omega) \quad (\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1$$

и которые обладают тем свойством, что четвертый и пятый коэффициенты формы, которая является дополнительной к той, в которую переходит форма  $f$  при подстановке  $(S)$

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'', \end{array}$$

соответственно равны  $\mathfrak{B}, \mathfrak{B}'$ . Именно, если положить

$$\pm B = \mathfrak{B} + \eta D, \quad \pm B' = \mathfrak{B}' + \zeta D$$

(где и здесь и дальше нужно брать верхние или нижние знаки в зависимости от того, эквивалентны значения  $(B, B'), (\mathfrak{B}, \mathfrak{B}')$  или противоположны), так что  $\zeta, \eta$  будут целыми числами, и если  $g$  при подстановке

$$\begin{array}{ccc} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{array}$$

переходит в форму  $g$ , то легко видеть, что ее определитель равен  $\Delta$ , а четвертый и пятый коэффициенты дополнительной формы равны соответственно  $\mathfrak{B}, \mathfrak{B}'$ . Если же положить

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta'',$$

то без труда получится, что  $f$  при подстановке  $(S)$  переходит в  $g$ , и что уравнение  $(\Omega)$  удовлетворяется.

Из этих принципов выводится следующий метод для отыскания всех собственных представлений двойничной формы

$$\varphi = pt^2 + 2qtu + ru^2$$

с определителем  $D$  тройничной формой  $f$  с определителем  $\Delta$ .



I. Найдем все различные (т. е. не эквивалентные) значения выражения  $\sqrt{\Delta(p, -q, r)} \pmod{D}$ . Для случая, когда  $\varphi$  является примитивной формой, и  $\Delta$  взаимно просто с  $D$ , эта задача была решена выше (п. 233), а остальные случаи очень легко могут быть сведены к этому, что мы, однако, подробнее выяснять ради краткости не будем. Заметим только, что если  $\Delta$  взаимно просто с  $D$ , то выражение  $\Delta(p, -q, r)$  не может быть квадратичным вычетом по модулю  $D$ , если  $\varphi$  не является приведенной формой. Действительно, если мы предположим, что

$$\Delta p = B^2 - DA', \quad -\Delta q = BB' - DB'', \quad \Delta r = B'^2 - DA,$$

то

$$(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r),$$

и отсюда, после раскрытия скобок и замены  $D$  на  $q^2 - pr$ , получается

$$(q^2 - pr)(B''^2 - AA') - \Delta(Ap + 2B''q + A'r) + \Delta^2 = 0,$$

откуда легко следует, что если бы числа  $p, q, r$  имели общий делитель, то он входил бы также и в  $\Delta^2$ ; но тогда  $\Delta$  не могло бы быть взаимно просто с  $D$ . Поэтому  $p, q, r$  не могут иметь общих делителей, т. е. форма  $\varphi$  является примитивной формой.

II. Если мы обозначим количество этих значений через  $m$  и предположим, что среди них имеется  $n$  значений, которые противоположны самим себе (причем мы полагаем  $n = 0$ , если таких значений нет), то ясно, что остальные  $m - n$  значений попарно противоположны (так как мы ведь предполагаем, что берутся все значения без исключения); если из каждой двух противоположных значений одно (любое) отбрасывается, то всего остается  $(m + n)/2$  значений. Так, например, из следующих восьми значений выражения  $\sqrt{-1(19, -3, 41)} \pmod{770}$ :  $(39, 237)$ ,  $(171, -27)$ ,  $(269, -83)$ ,  $(291, -127)$ ,  $(-39, -237)$ ,  $(-171, 27)$ ,  $(-269, 83)$ ,  $(-291, 127)$  — последние четыре надо отбросить, так как они противоположны четырем первым. Впрочем, очевидно, что если  $(B, B')$  есть значение, противоположное самому себе, то  $2B, 2B'$ , а потому также и  $2\Delta p, 2\Delta q, 2\Delta r$  делятся на  $D$ ; поэтому если  $\Delta$  и  $D$  взаимно просты, то  $2p, 2q, 2r$  будут также делиться на  $D$ , а так

как, согласно I,  $p, q, r$  не могут иметь общих делителей, то на  $D$  должно будет делиться число 2, что возможно только тогда, когда либо  $D = \pm 1$ , либо  $D = \pm 2$ . Поэтому для всех значений  $D$ , которые больше чем 2, всегда  $n = 0$ , если  $\Delta$  взаимно просто с  $D$ .

III. Теперь ясно, что каждое собственное представление формы  $\varphi$  формой  $f$  обязательно должно принадлежать к некоторому из оставшихся значений, причем только к одному. Поэтому нужно брать последовательно эти значения и для каждого из них находить принадлежащие им представления. Чтобы найти представления, принадлежащие заданному значению  $(B, B')$ , нужно сначала определить тройничную форму  $g = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$ , определитель которой равен  $\Delta$  и у которой  $a = p, b'' = q, a' = r, ab - b'b'' = B, a'b' - bb'' = B'$ ; значения  $a'', b, b'$  находятся отсюда при помощи равенств из п. 276, II, из которых легко видно, что в случае, когда  $\Delta, D$  взаимно просты, числа  $b, b', a''$  будут целыми (именно, потому, что эти три числа дают целые числа при умножении как на  $D$ , так и на  $\Delta$ ). Если теперь либо один из коэффициентов  $b, b', a''$  дробный, либо формы  $f, g$  не эквивалентны, то не может быть принадлежащих значению  $(B, B')$  представлений формы  $\varphi$  формой  $f$ ; если же числа  $b, b', a''$  целые и формы  $f, g$  эквивалентны, то каждое преобразование первой во вторую, например, преобразование

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

дает одно такое представление, именно,

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u,$$

и, очевидно, не может быть такого представления, которое не могло бы быть выведено из некоторого преобразования. Таким образом, та часть второй задачи, которая ставит себе целью разыскание *собственных* представлений, уже сведена к третьей задаче.

IV. Далее, из различных преобразований формы  $f$  в форму  $g$  всегда получаются различные представления, за исключением единственного случая, когда значение  $(B, B')$  противоположно

самому себе и когда по два преобразования дают одно и то же представление. Именно, если мы предположим, что  $f$  переходит в  $g$  при подстановке

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{array}$$

(которая дает то же представление, что и предыдущее преобразование) и обозначим через  $k, \mathfrak{k}, \zeta, \eta$  те же числа, что и во втором разделе предыдущего пункта, то

$$B = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D;$$

если поэтому оба числа  $k, \mathfrak{k}$  положить либо равными  $+1$ , либо равными  $-1$ , то (так как мы исключили случай  $D = 0$ ) будет иметь место  $\zeta = 0, \eta = 0$ , откуда легко следует, что  $\delta = \gamma, \delta' = \gamma', \delta'' = \gamma''$ . Поэтому оба наши преобразования могут быть различны только в том случае, когда одно из чисел  $\mathfrak{k}, k$  равно  $+1$ , а другое равно  $-1$ ; тогда  $B \equiv -B, B' \equiv -B' \pmod{D}$ , т. е. значение  $(B, B')$  противоположно самому себе.

V. Из того, что выше (п. 271) мы указали относительно критериев определенных и неопределенных форм, легко видеть, что если  $\Delta$  положительно,  $D$  отрицательно, и  $\varphi$  является отрицательной формой, то  $g$  будет определенной отрицательной формой; если же  $\Delta$  положительно, и либо  $\Delta$  и  $D$  положительно, либо  $D$  отрицательно и форма  $\varphi$  положительна, то  $g$  будет неопределенной формой. Так как теперь  $f$  и  $g$  заведомо не могут быть эквивалентны, если они не однотипны в отношении этого свойства, то ясно, что двойничные формы с положительным определителем, так же, как и положительные формы, не могут быть собственно представлены тройничной отрицательной формой, и отрицательные двойничные формы — неопределенной тройничной формой с положительным определителем, а что, напротив, тройничной формой первого или второго типа могут собственно представляться только двойничные формы соответственно второго или первого типа. Аналогичным образом следует, что определенной (т. е. положительной) тройничной формой с отрицательным определителем могут представляться только положи-

тельные двойничные формы, а неопределенной тройничной формой — только отрицательные двойничные формы с положительным определителем.

284

Так как *несобственными* представлениями двойничной формы  $\varphi$  с определителем  $D$  тройничной формой  $f$ , дополнительной к которой является форма  $F$ , будут те, из которых получаются несобственные представления числа  $D$  формой  $F$ , то очевидно, что  $\varphi$  может быть представлена формой  $f$  только несобственно, если  $D$  содержит квадратные сомножители. Если мы предположим, что все входящие в  $D$  квадраты (кроме 1) суть  $e^2, e'^2, e''^2, \dots$  (их количество конечно, так как мы предполагаем, что  $D$  не равно 0), то каждое несобственное представление формы  $\varphi$  формой  $f$  будет, очевидно, приводить к представлению числа  $D$  формой  $F$ , у которого значения переменных имеют в качестве наибольшего общего делителя одно из чисел  $e, e', e'', \dots$ ; в этой связи мы ради краткости будем говорить, что каждое несобственное представление формы  $\varphi$  принадлежит квадратному делителю  $e^2$ , или  $e'^2$ , или  $e''^2$  и т. д. Но все представления формы  $\varphi$ , принадлежащие одному и тому же *заданному* квадратному делителю  $e^2$  (корень из которого,  $e$ , мы предполагаем положительным), находятся по следующим правилам, из синтетического доказательства которых, избранного нами здесь ради краткости, легко восстановить анализ, при помощи которого они были найдены.

*Сначала* нужно найти все двойничные формы с определителем  $D/e^2$ , которые переходят в форму  $\varphi$  при собственной подстановке вида  $T = \kappa t + \lambda u, U = \mu u$ , где  $T, U$  обозначают переменные такой формы,  $t, u$  — переменные формы  $\varphi$ ;  $\kappa, \mu$  — положительные целые числа (произведение которых тем самым равно  $e$ ) и  $\lambda$  — положительное число, которое меньше, чем  $\mu$  (включая и нуль). Эти формы вместе с соответствующими преобразованиями находятся следующим образом.

Будем придавать  $\kappa$  последовательно значения, равные отдельным положительным делителям числа  $e$  (включая 1 и  $e$ ), и полагать  $\mu = \frac{e}{\kappa}$ ; для отдельных определенных значений  $\kappa, \mu$  будем

придавать  $\lambda$  все целые значения от 0 до  $\mu - 1$ , благодаря чему мы заведомо получим все преобразования. Тогда мы найдем форму, которая при подстановке  $T = \kappa t + \lambda u$ ,  $U = \mu u$  переходит в  $\varphi$ , если разыщем форму, в которую переходит  $\varphi$  при подстановке  $t = \frac{1}{\kappa} T - \frac{\lambda}{e} U$ ,  $u = \frac{1}{\mu} U$ ; таким образом мы получим формы, соответствующие отдельным преобразованиям; однако из всех этих форм нужно оставить только те, у которых все три коэффициента будут целыми числами \*.

*Во-вторых*, предполагая, что  $\Phi$  — какая-нибудь из этих форм, которая переходит в  $\varphi$  при подстановке  $T = \kappa t + \lambda u$ ,  $U = \mu u$ , найдем все собственные представления формы  $\Phi$  формой  $f$  (если таковые имеются) и выразим их в общем виде формулами

$$(\mathfrak{K}) \quad x = \mathfrak{A}T + \mathfrak{B}U, \quad x' = \mathfrak{A}'T + \mathfrak{B}'U, \quad x'' = \mathfrak{A}''T + \mathfrak{B}''U;$$

наконец, из каждого отдельного представления  $(\mathfrak{K})$  выведем представление

$$(\rho) \quad x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

посредством равенств

$$(R) \quad \begin{cases} \alpha = \kappa \mathfrak{A}, & \alpha' = \kappa \mathfrak{A}', & \alpha'' = \kappa \mathfrak{A}'', \\ \beta = \lambda \mathfrak{A} + \mu \mathfrak{B}, & \beta' = \lambda \mathfrak{A}' + \mu \mathfrak{B}', & \beta'' = \lambda \mathfrak{A}'' + \mu \mathfrak{B}''. \end{cases}$$

Совершенно таким же образом, как и форму  $\Phi$ , рассмотрим и остальные формы, найденные по первому правилу (если их несколько), так что из отдельных собственных представлений получатся все другие представления; тогда, как я утверждаю, таким путем будут найдены все принадлежащие делителю  $e^2$  представления формы  $\varphi$ , и притом каждое получится только один раз.

**Доказательство.** I. То, что тройничная форма  $f$  при каждой подстановке  $(\rho)$  действительно переходит в  $\varphi$ , настолько ясно, что

---

\* Если бы мы могли здесь более подробно рассмотреть этот вопрос, нам удалось бы существенно сократить решение. Непосредственно ясно, что в качестве  $\kappa$  нет нужды брать никаких других делителей числа  $e$ , кроме тех, квадраты которых входят в первый коэффициент формы  $\varphi$ . Впрочем, при другом удобном случае мы еще вернемся к этой проблеме, из решения которой также могут быть получены более простые решения проблем пп. 213, 214.

не требует дальнейшего пояснения; а то, что каждое представление  $(\rho)$  является несобственным и принадлежит делителю  $e^2$ , вытекает из того, что числа  $\alpha'\beta'' - \alpha''\beta'$ ,  $\alpha''\beta - \alpha\beta''$ ,  $\alpha\beta' - \alpha'\beta$  будут равны соответственно  $e(\mathfrak{U}'\mathfrak{B}'' - \mathfrak{U}''\mathfrak{B}')$ ,  $e(\mathfrak{U}''\mathfrak{B} - \mathfrak{U}\mathfrak{B}'')$ ,  $e(\mathfrak{U}\mathfrak{B}' - \mathfrak{U}'\mathfrak{B})$ , вследствие чего их наибольшим общим делителем, очевидно, является  $e$  (так как представление  $(\mathfrak{K})$  собственное).

II. Мы покажем, что из каждого заданного представления  $(\rho)$  формы  $\phi$  может быть найдено собственное представление формы с определителем  $D/e^2$ , которое содержится среди представлений, найденных по первому правилу, т. е. что из заданных значений  $\alpha$ ,  $\alpha'$ ,  $\alpha''$ ,  $\beta$ ,  $\beta'$ ,  $\beta''$  могут быть выведены целочисленные значения  $\kappa$ ,  $\lambda$ ,  $\mu$ , которые удовлетворяют предписанным условиям, и значения  $\mathfrak{U}$ ,  $\mathfrak{U}'$ ,  $\mathfrak{U}''$ ,  $\mathfrak{B}$ ,  $\mathfrak{B}'$ ,  $\mathfrak{B}''$ , которые удовлетворяют равенствам  $(R)$ , и притом только одним единственным образом. Действительно, прежде всего из первых трех равенств в  $(R)$  вытекает, что за  $\kappa$  должен быть взят наибольший общий делитель чисел  $\alpha$ ,  $\alpha'$ ,  $\alpha''$  с положительным знаком (именно так как  $\mathfrak{U}'\mathfrak{B}'' - \mathfrak{U}''\mathfrak{B}'$ ,  $\mathfrak{U}''\mathfrak{B} - \mathfrak{U}\mathfrak{B}''$ ,  $\mathfrak{U}\mathfrak{B}' - \mathfrak{U}'\mathfrak{B}$  не имеют общих делителей, то и  $\mathfrak{U}$ ,  $\mathfrak{U}'$ ,  $\mathfrak{U}''$  не могут иметь общих делителей); тем самым определяются и  $\mathfrak{U}$ ,  $\mathfrak{U}'$ ,  $\mathfrak{U}''$ , а также и  $\mu = \frac{e}{\kappa}$  (легко видеть, что это число обязательно целое). Если мы предположим, что три целых числа  $\alpha$ ,  $\alpha'$ ,  $\alpha''$  выбраны так, что  $\alpha\mathfrak{U} + \alpha'\mathfrak{U}' + \alpha''\mathfrak{U}'' = 1$ , и ради краткости вместо  $\alpha\mathfrak{B} + \alpha'\mathfrak{B}' + \alpha''\mathfrak{B}''$  будем писать  $k$ , то из последних трех равенств  $(R)$  следует, что  $\alpha\beta + \alpha'\beta' + \alpha''\beta'' = \lambda + \mu k$ , откуда тотчас же вытекает, что для  $\lambda$  имеется только одно значение между 0 и  $\mu - 1$ . Но так как после того, как это сделано,  $\mathfrak{B}$ ,  $\mathfrak{B}'$ ,  $\mathfrak{B}''$  тоже получают определенные значения, нам остается только еще доказать, что они всегда будут целыми. Но

$$\begin{aligned}\mathfrak{B} &= \frac{1}{\mu} (\beta - \lambda\mathfrak{U}) = \frac{1}{\mu} [\beta (1 - \alpha\mathfrak{U}) - \mathfrak{U} (\alpha'\beta' - \alpha''\beta'')] + \mathfrak{U}k = \\ &= \frac{1}{\mu} [\alpha'' (\mathfrak{U}''\beta - \mathfrak{U}\beta'') - \alpha' (\mathfrak{U}\beta' - \mathfrak{U}'\beta)] + \mathfrak{U}k = \\ &= \frac{1}{e} [\alpha'' (\alpha''\beta - \alpha\beta'') - \alpha' (\alpha\beta' - \alpha'\beta)] + \mathfrak{U}k,\end{aligned}$$

и потому  $\mathfrak{B}$ , очевидно, является целым числом, и точно так же

устанавливается, что и  $\mathfrak{B}'$ ,  $\mathfrak{B}''$  получают целочисленные значения. Из этих рассуждений следует, что не может быть несобственного представления формы  $\varphi$  формой  $f$ , принадлежащего делителю  $e^2$ , которое указанным методом могло бы либо не получиться вовсе, либо получиться несколько раз.

Если теперь таким же образом исследовать остальные квадратные делители числа  $D$  и найти представления, принадлежащие каждому из них, то мы получим все несобственные представления формы  $\varphi$  формой  $f$ .

Далее, из этого решения легко получается, что указанная в конце предыдущего пункта теорема относительно собственных представлений имеет силу и для несобственных представлений, а именно, что вообще никакая положительная двойничная форма с отрицательным определителем не может быть представлена отрицательной тройничной формой и т. д. Действительно, если  $\varphi$  есть такая двойничная форма, которая, в силу указанной теоремы не может быть представлена формой  $f$  собственно, то очевидно, что и все формы с определителями  $D/e^2$ ,  $D/e'^2, \dots$ , которые содержат форму  $\varphi$ , не могут быть собственно представлены формой  $f$ , так как все эти формы имеют определители того же знака, что и определитель формы  $\varphi$ , и если эти определители отрицательны, то либо все формы будут положительны, либо все отрицательны в зависимости от того, принадлежит ли  $\varphi$  к первым или ко вторым.

## 285

Относительно вопросов, которые образуют третью из поставленных нами проблем (к которой в предыдущем сведены обе первые проблемы), а именно, если заданы две тройничные формы с одним и тем же определителем, узнать, эквивалентны они или нет, и в первом случае найти все преобразования одной из них в другую, мы можем в этом месте сказать только немного, так как полное решение, которое мы указали для аналогичной проблемы в случае двойничных форм, здесь наталкивается на еще бóльшие трудности. Поэтому мы ограничим наше исследование некоторыми специальными случаями, ради которых мы главным образом и предприняли это отступление от нашего основного предмета.

I. Выше было показано, что для определителя  $+1$  все тройничные формы распадаются на два класса, один из которых содержит все неопределенные формы, а другой — все определенные (отрицательные) формы. Из этого тотчас же следует, что любые две тройничные формы с определителем  $1$  эквивалентны, если либо обе они определенные, либо обе неопределенные; если же одна из них определенная, а другая неопределенная, то эквивалентность не может иметь места (вторая часть теоремы, очевидно, справедлива вообще для форм с любым определителем). Точно так же некоторые две формы с определителем  $-1$  заведомо будут эквивалентны, если либо обе они определенные, либо обе неопределенные. Две определенные формы с определителем  $2$  всегда будут эквивалентны; две неопределенные формы не будут эквивалентны, если у одной из них первые три коэффициента все четны, а у другой — не все четны; в остальных случаях (когда три первые коэффициента все одновременно четны либо у обеих форм, либо ни у одной из них) они, напротив, будут эквивалентны. Таким же образом мы могли бы установить еще намного больше специальных теорем, если бы выше (п. 277) исследовали больше примеров.

II. Во всех этих случаях, если  $f, f'$  обозначают тройничные эквивалентные формы, можно найти также *одно* преобразование одной из них в другую. Действительно, для всех случаев в каждом классе тройничных форм выше было указано достаточно маленькое число форм, к которым вполне определенным методом может быть сведена любая форма этого класса; там же было показано, как можно все эти формы привести к одной. Если  $F$  — это форма в том классе, которому принадлежат  $f, f'$ , то при помощи указанных выше правил могут быть найдены преобразования форм  $f, f'$  в  $F$  и точно так же преобразования формы  $F$  в  $f, f'$ . Отсюда, согласно п. 270, могут быть выведены преобразования формы  $f$  в  $f'$  и формы  $f'$  в  $f$ .

III. Поэтому остается только показать, как из *одного* преобразования одной тройничной формы  $f$  в другую форму  $f'$  можно вывести все возможные преобразования. Эта задача сводится к более простой, а именно, найти все преобразования тройничной формы  $f$  в себя. Именно, если  $f$  при нескольких подстановках  $(\tau), (\tau'), (\tau''), \dots$  переходит сама в себя, а при подстановке  $(t)$  — в  $f'$ , то если комбиниро-



вать, как было указано в п. 270, преобразование  $(t)$  с  $(\tau)$ ,  $(\tau')$ ,  $(\tau'')$ , ..., будут, очевидно, все время получаться подстановки, при которых  $f$  переходит в  $f'$ ; кроме того, выкладкой легко устанавливается, что каждое преобразование формы  $f$  в  $f'$  может быть получено таким путем из комбинации заданного преобразования  $(t)$  формы  $f$  в  $f'$  с некоторым (и притом только одним) преобразованием формы  $f$  в себя, и что тем самым из комбинаций заданного преобразования формы  $f$  в  $f'$  со всеми преобразованиями формы  $f$  в себя получаются все преобразования формы  $f$  в  $f'$ , и притом каждое только один раз.

Отыскание всех преобразований формы  $f$  в себя мы ограничим здесь случаем, когда  $f$  является определенной формой, у которой четвертый, пятый и шестой коэффициенты все равны 0 \*. Пусть поэтому  $f = \begin{pmatrix} a, & a' & a'' \\ 0, & 0, & 0 \end{pmatrix}$ , и пусть произвольная подстановка, при которой  $f$  переходит в себя, обозначена через

$$\begin{aligned} &\alpha, \beta, \gamma \\ &\alpha', \beta', \gamma' \\ &\alpha'', \beta'', \gamma'', \end{aligned}$$

так что должны удовлетворяться равенства

$$(\Omega) \quad \begin{cases} a\alpha^2 + a'\alpha'^2 + a''\alpha''^2 = a, \\ a\beta^2 + a'\beta'^2 + a''\beta''^2 = a', \\ a\gamma^2 + a'\gamma'^2 + a''\gamma''^2 = a'', \\ a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' = 0, \\ a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' = 0, \\ a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' = 0. \end{cases}$$

Теперь нужно различать три случая.

I. Если числа  $a$ ,  $a'$ ,  $a''$  (которые имеют одинаковые знаки) все различны между собой, то мы предположим, что  $a < a'$ ,  $a' < a''$  (если бы расположение по величине было другим, то можно было бы получить те же выводы совершенно аналогичным образом). Тогда

---

\* Остальные случаи, когда  $f$  является определенной формой, сводятся к этому; если же форма  $f$  неопределенная, то нужно применять совсем другой метод, и количество преобразований оказывается бесконечно большим.

первое из равенств ( $\Omega$ ), очевидно, дает, что  $\alpha' = \alpha'' = 0$ , и потому  $\alpha = \pm 1$ ; поэтому из четвертого и пятого равенств следует  $\beta = 0$ ,  $\gamma = 0$ ; аналогично, из второго равенства получается  $\beta'' = 0$ , и потому  $\beta = \pm 1$ , а затем из шестого равенства  $\gamma' = 0$  и из третьего  $\gamma'' = \pm 1$ , так что мы получаем (за счет независимых друг от друга двойных знаков) восемь различных преобразований.

II. Если из чисел  $a, a', a''$  два равны одно другому, например,  $a' = a''$ , а третье отлично от них, то мы предположим следующее.

Во-первых, что  $a < a'$ . Тогда таким же образом, как и в предыдущем случае, получается, что  $\alpha' = 0$ ,  $\alpha'' = 0$ ,  $\alpha = \pm 1$ ,  $\beta = 0$ ,  $\gamma = 0$ ; а из второго, третьего и шестого равенств легко видеть, что либо  $\beta' = \pm 1$ ,  $\gamma' = 0$ ,  $\beta'' = 0$ ,  $\gamma'' = \pm 1$ , либо  $\beta' = 0$ ,  $\gamma' = \pm 1$ ,  $\beta'' = \pm 1$ ,  $\gamma'' = 0$ .

Если же, во-вторых,  $a > a'$ , то мы получаем те же результаты следующим образом. Из второго и третьего равенств следует обязательно, что  $\beta = 0$ ,  $\gamma = 0$ , и либо  $\beta' = \pm 1$ ,  $\gamma' = 0$ ,  $\beta'' = 0$ ,  $\gamma'' = \pm 1$ , либо  $\beta' = 0$ ,  $\gamma' = \pm 1$ ,  $\beta'' = \pm 1$ ,  $\gamma'' = 0$ . При обоих предположениях из четвертого и пятого равенств следует, что  $\alpha' = 0$ ,  $\alpha'' = 0$ , а из первого, — что  $\alpha = \pm 1$ . Поэтому в каждом случае имеется шестнадцать различных преобразований. Оба других случая, в которых либо  $a = a''$ , либо  $a = a'$ , разбираются совершенно аналогичным образом, если только заменить буквы  $\alpha, \alpha', \alpha''$  в первом случае соответственно буквами  $\beta, \beta', \beta''$ , а во втором — буквами  $\gamma, \gamma', \gamma''$ .

III. Если все три числа  $a, a', a''$  равны между собой, то из первых двух равенств вытекает, что среди трех чисел  $\alpha, \alpha', \alpha''$ , так же, как и среди чисел  $\beta, \beta', \beta''$  и  $\gamma, \gamma', \gamma''$ , по два числа равны 0, а третье равно  $\pm 1$ . Но из трех последних равенств легко усмотреть, что из трех чисел  $\alpha, \beta, \gamma$  может быть равно  $\pm 1$  только одно, и так же обстоит дело для чисел  $\alpha', \beta', \gamma'$  и  $\alpha'', \beta'', \gamma''$ . Поэтому всего имеется только шесть комбинаций:

$$\begin{array}{c|c|c|c|c|c|c} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array} ;$$

все остальные коэффициенты  $= 0$ ,

так что за счет двойных знаков всего мы получаем 48 преобразований. Эта же схема охватывает также и предыдущие случаи; но из шести колонок нужно брать только первую, если все числа  $a$ ,  $a'$ ,  $a''$  различны; первую и вторую колонки, если  $a' = a''$ , первую и третью, если  $a = a'$ , и первую и шестую, если  $a = a''$ .

Отсюда получается, что если тройничная форма  $f = ax^2 + a'x'^2 + a''x''^2$  переходит в другую эквивалентную ей форму  $f'$  при подстановке

$$x = \delta y + \varepsilon y' + \zeta y'', \quad x' = \delta' y + \varepsilon' y' + \zeta' y'', \quad x'' = \delta'' y + \varepsilon'' y' + \zeta'' y'',$$

то все преобразования формы  $f$  в  $f'$  содержатся в следующей схеме:

|       |       |       |       |       |       |                                                       |
|-------|-------|-------|-------|-------|-------|-------------------------------------------------------|
| $x$   | $x$   | $x'$  | $x'$  | $x''$ | $x''$ | $= \pm (\delta y + \varepsilon y' + \zeta y'')$       |
| $x'$  | $x''$ | $x$   | $x''$ | $x$   | $x'$  | $= \pm (\delta' y + \varepsilon' y' + \zeta' y'')$    |
| $x''$ | $x'$  | $x''$ | $x$   | $x'$  | $x$   | $= \pm (\delta'' y + \varepsilon'' y' + \zeta'' y'')$ |

с учетом того, что нужно использовать все шесть колонок, если  $a = a' = a''$ , первую и вторую колонки, если  $a'$ ,  $a''$  равны между собой, а  $a$  отлично от них, первую и третью, если  $a = a'$ , первую и шестую, если  $a = a''$ , наконец, только первую колонку, если все числа  $a$ ,  $a'$ ,  $a''$  различны между собой. В первом случае количество преобразований равно 48, во втором, третьем и четвертом случае равно 16 и в пятом — равно 8.

## НЕКОТОРЫЕ ПРИЛОЖЕНИЯ К ТЕОРИИ ДВОЙНИЧНЫХ ФОРМ

### Об отыскании формы, при удвоении которой получается заданная двойничная форма главного рода

От этого краткого изложения первых элементов теории тройничных форм мы переходим к некоторым специальным приложениям, из которых на первом месте стоит следующая проблема.

**Задача.** Пусть дана принадлежащая главному роду двойничная форма  $F = (A, B, C)$  с определителем  $D$ ; нужно найти двойничную форму  $f$ , при удвоении которой получается форма  $F$ .

**Решение.** I. Найдем собственное представление противоположной форме  $F$  формы  $F' = AT^2 - 2BTU + CU^2$  тройничной формой  $x^2 - 2yz$  пусть это представление таково:

$$x = \alpha T + \beta U, \quad y = \alpha' T + \beta' U, \quad z = \alpha'' T + \beta'' U.$$

То, что это возможно сделать, легко следует из предшествующей теории тройничных форм. Действительно, так как, по предположению, форма  $F$  принадлежит главному роду, то существует значение выражения  $\sqrt{(A, B, C)} \pmod{D}$ , вследствие чего может быть найдена тройничная форма  $\varphi$  с определителем 1, в которую форма  $(A, -B, C)$  входит как часть, причем легко убедиться, что все коэффициенты этой формы являются целыми числами. Так же легко видеть, что  $\varphi$  является неопределенной формой (так как, по предположению,  $F$  заведомо не является отрицательной формой); поэтому она обязательно эквивалентна форме  $x^2 - 2yz$ . Следовательно, можно найти собственное преобразование второй формы в первую, которое даст собственное представление формы  $F$  формой  $x^2 - 2yz$ .

Итак, мы имеем

$$A = \alpha^2 - 2\alpha'\alpha'', \quad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \quad C = \beta^2 - 2\beta'\beta'';$$

если, далее, обозначить числа  $\alpha\beta' - \alpha'\beta$ ,  $\alpha'\beta'' - \alpha''\beta'$ ,  $\alpha''\beta - \alpha\beta''$  соответственно через  $a$ ,  $b$ ,  $c$ , то они не будут иметь общих делителей, и, кроме того,  $D = b^2 - 2ac$ .

II. Из этого при помощи последнего замечания из п. 235 легко выводится, что форма  $F$  при подстановке  $2\beta'$ ,  $\beta$ ,  $\beta$ ,  $\beta''$ ;  $2\alpha'$ ,  $\alpha$ ,  $\alpha$ ,  $\alpha''$  переходит в произведение формы  $(2a, -b, c)$  на себя самое, и точно так же при подстановке  $\beta'$ ,  $\beta$ ,  $\beta$ ,  $2\beta''$ ;  $\alpha'$ ,  $\alpha$ ,  $\alpha$ ,  $2\alpha''$  — в произведение на самое себя формы  $(a, -b, 2c)$ . Наибольший общий делитель чисел  $2a$ ,  $2b$ ,  $2c$  равен 2; поэтому если  $c$  нечетно, то числа  $2a$ ,  $2b$ ,  $c$  не будут иметь общих делителей, т. е. форма  $(2a, -b, c)$  будет собственно примитивной; точно так же, если нечетно  $a$ , то будет

собственно примитивной форма  $(a, -b, 2c)$ . В первом случае форма  $F$  получается при удвоении формы  $(2a, -b, c)$ , а во втором — при удвоении формы  $(a, -b, 2c)$  (ср. четвертое следствие п. 235); но всегда заведомо будет иметь место один из этих случаев. Действительно, если бы оба числа  $a, c$  были четны, то  $b$  обязательно было бы нечетным; но легко убедиться, что  $\beta''a + \beta b + \beta'c = 0$ ,  $\alpha''a + \alpha b + \alpha'c = 0$ , из чего следовало бы, что являются четными числа  $\beta b, \alpha b$ , а потому также и  $\alpha, \beta$ . Вследствие этого  $A$  и  $C$  были бы четными, что противоречит предположению о том, что форма  $F$  принадлежит главному роду. и, следовательно, собственно примитивному порядку.

Возможно также, что будут нечетными оба числа  $a$  и  $c$ ; в этом случае мы имеем тем самым две формы, при удвоении которых получается форма  $F$ .

**Пример.** Пусть дана форма  $F = (5, 2, 31)$  с определителем  $-151$ . В качестве значения выражения  $\sqrt{(5, 2, 31)}$  находим здесь  $(55, 22)$ , откуда получается тройничная форма  $\varphi = \begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix}$ ; по правилам, указанным в п. 272, получаем эквивалентную ей форму  $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ , которая переходит в форму  $\varphi$  при подстановке

$$\begin{array}{ccc} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1. \end{array}$$

Отсюда при помощи указанных в п. 277 преобразований следует, что форма  $\begin{pmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{pmatrix}$  переходит в форму  $\varphi$  при подстановке

$$\begin{array}{ccc} 3, & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3. \end{array}$$

Поэтому  $a = 11$ ,  $b = -17$ ,  $c = 20$ ; следовательно, так как  $a$  нечетно, форма  $F$  получается при удвоении формы  $(11, 17, 40)$  и переходит в произведение этой формы на самое себя при подстановке  $-1, -7, -7, -18; 2, 3, 3, 2$ .

**Всем характеристам, за исключением тех,  
невозможность которых была доказана в пп. 263, 264,  
действительно соответствуют роды**

287

*Относительно решенной в предыдущем пункте задачи мы добавим еще следующие замечания.*

I. Если форма  $F$  при подстановке  $p, p', p'', p'''; q, q', q'', q'''$  переходит в произведение двух форм  $(h, i, k), (h', i', k')$  (каждая из которых, как мы всегда предполагаем, берется собственно), то имеют место легко выводимые из третьего следствия п. 235 равенства:

$$\begin{aligned} p''hn' - p'h'n - p(in' - i'n) &= 0, \\ (p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) &= 0, \\ p'kn' - p''k'n - p'''(in' - i'n) &= 0, \end{aligned}$$

и три других равенства, которые получаются из этих заменой чисел  $p, p', p'', p'''$  на  $q, q', q'', q'''$ ; числа  $n, n'$  являются положительными квадратными корнями из частных, которые получаются, если определители форм  $(h, i, k), (h', i', k')$  разделить на определитель формы  $F$ . Если же эти две формы совпадают, т. е.  $n = n', h = h', i = i', k = k'$ , то указанные равенства переходят в следующие:

$$(p'' - p')hn = 0, \quad (p'' - p')in = 0, \quad (p'' - p')kn = 0,$$

откуда получается, что обязательно  $p' = p''$ , и, совершенно аналогичным образом,  $q' = q''$ . Таким образом, если формы  $(h, i, k), (h', i', k')$  зависят от одних и тех же переменных,  $t, u$ , а переменные формы  $F$  обозначены через  $T, U$ , то  $F$  будет переходить в  $(ht^2 + 2itu + ku^2)^2$  при подстановке

$$T = pt^2 + 2p'tu + p''u^2, \quad U = qt^2 + 2q'tu + q''u^2.$$

II. Если форма  $F$  получается удвоением формы  $f$ , то она будет получаться и при удвоении всякой другой формы, содержащейся в одном классе с  $f$ , т. е. класс формы  $F$  будет получаться удвоением класса формы  $f$  (ср. п. 238). Так, в примере предыдущего пункта форма  $(5, 2, 31)$  получается также и удвоением формы  $(11, -5, 16)$ ,

которая собственно эквивалентна форме (11, 17, 40). Из одного класса, при удвоении которого получается класс формы  $F$ , все остальные такие классы (если их имеется несколько) находятся на основании изложенного в п. 260; в нашем примере других положительных классов такого сорта нет, так как существует только один двусторонний собственно примитивный положительный класс с определителем  $-151$  (именно, главный класс); так как при композиции единственного двустороннего отрицательного класса  $(-1, 0, -151)$  с классом  $(11, -5, 16)$  получается класс  $(-11, -5, -16)$ , то он и будет единственным отрицательным классом, при удвоении которого получается класс  $(5, 2, 31)$ .

III. Так как благодаря решению задачи предыдущего пункта установлено, что каждый собственно примитивный (положительный) принадлежащий главному роду класс двойничных форм может быть получен удвоением некоторого собственно примитивного класса с тем же определителем, то теорема п. 261, утверждающая, что по крайней мере половине всех возможных для данного неквадратного определителя  $D$  характеров не могут соответствовать собственно примитивные положительные роды, может быть теперь усилена утверждением, что *в действительности такие роды соответствуют в точности половине всех этих характеров*, другой же их половине такие роды тем самым соответствовать не могут (ср. доказательство указанной теоремы). Если в п. 264 все возможные характеры были разбиты на две равных совокупности  $P$ ,  $Q$ , причем для характеров из совокупности  $Q$  было доказано, что им не могут соответствовать собственно примитивные положительные формы, в то время как для характеров из  $P$  оставалось неясным, действительно ли каждому из них соответствуют такие роды, то теперь эта неясность полностью устранена, и мы можем быть уверены, что во всей совокупности  $P$  нет ни одного характера, которому не соответствовал бы некоторый род. Но отсюда легко выводится также и то, что для отрицательного определителя в отрицательном собственно примитивном порядке, в котором, как мы показали в п. 264, I, невозможны все характеры из  $P$ , а возможны лишь характеры из  $Q$ , в действительности возможны все характеры из  $Q$ . Именно, если обозначить через  $K$  какой-нибудь характер из  $Q$ , через  $f$  — любую форму из

отрицательного собственно примитивного порядка форм с определителем  $D$  и через  $K'$  — ее характер, то последний будет содержаться в  $Q$ , откуда легко следует, что характер, составленный из  $K, K'$  (по правилу п. 246), принадлежит совокупности  $P$ , и потому существуют положительные собственно примитивные формы с определителем  $D$ , которые ему соответствуют; при композиции любой из таких форм с формой  $f$  получается, очевидно, отрицательная собственно примитивная форма с определителем  $D$ , характером которой является  $K$ . Совершенно аналогичным образом показывается, что в несобственно примитивном порядке все те характеры, которые, согласно правилам п. 264, II, III, только и могут быть возможны, оказываются действительно возможными, независимо от того, содержатся ли они в  $P$  или в  $Q$ . Эти теоремы, если мы не слишком заблуждаемся, следует причислить к прекраснейшим теоремам теории двойничных форм, тем более, что хотя они имеют совсем простую природу, но скрыты так глубоко, что строгое доказательство их невозможно без помощи такого большого числа других исследований.

### Теория разложения чисел и двойничных форм на три квадрата

Теперь мы переходим к другому приложению предыдущего отступления, а именно, к разложению чисел и двойничных форм на три квадрата, причем предположим этому следующую задачу \*.

288

**Задача.** Пусть  $M$  обозначает положительное число; найти условия, при которых существуют отрицательные примитивные двойничные формы с определителем  $-M$ , которые являются квадратичными вычетами числа  $M$ , т. е. для которых 1 является характеристическим числом.

**Решение.** Обозначим через  $\Omega$  совокупность всех специальных характеров, которые указывают отношения числа 1 как к отдельным

---

\* Ср. дополнения в конце «Исследований».



(нечетным) простым делителям числа  $M$ , так и к числам 8 или 4, если они входят в  $M$ ; очевидно, что этими характерами будут  $Rp$ ,  $Rp'$ ,  $Rp''$ , ..., где  $p$ ,  $p'$ ,  $p''$ , ... обозначают упомянутые простые делители, и 1, 4 или 1, 8, если в  $M$  входит соответственно число 4 или число 8. Далее, будем использовать буквы  $P$ ,  $Q$ , в том же значении, что и в предыдущем пункте, или в п. 264. *Теперь мы будем различать следующие случаи.*

I. Если  $M$  делится на 4, то  $\Omega$  является полным характером и из п. 233, V вытекает, что 1 может быть характеристическим числом только тех форм, характером которых является  $\Omega$ . Но очевидно, что  $\Omega$  является характером главной формы  $(1, 0, M)$  и принадлежит тем самым совокупности  $P$ , а, значит, не может соответствовать никакой отрицательной собственно примитивной форме; поскольку несобственно примитивных форм для такого определителя нет, в этом случае вообще не существует отрицательных примитивных форм, которые являются вычетами числа  $M$ .

II. Если  $M \equiv 3 \pmod{4}$ , то рассуждения остаются теми же, за единственным исключением, что в этом случае существует *несобственно* примитивный отрицательный порядок, в котором характеры из  $P$  либо возможны, либо нет, в зависимости от того, имеет ли место  $M \equiv 3$  или  $\equiv 7 \pmod{8}$  (ср. п. 264, III). В первом случае в этом порядке существует, следовательно, род, характером которого является  $\Omega$ , вследствие чего 1 будет характеристическим числом всех форм из этого рода; во втором случае вообще не существует отрицательных форм, обладающих этим свойством.

III. Если  $M \equiv 1 \pmod{4}$ , то  $\Omega$  еще не является полным характером, так как к нему нужно добавить еще отношение к числу 4; очевидно, однако, что  $\Omega$  обязательно должно входить в характер формы, для которой 1 является характеристическим числом, и, наоборот, каждое число, характером которого является либо  $\Omega$ ; 1, 4, либо  $\Omega$ ; 3, 4, должно иметь характеристическое число 1. Но  $\Omega$ ; 1, 4 является, очевидно, характером главного рода, принадлежащим к  $P$ , и потому в отрицательном собственно примитивном порядке невозможным; по той же причине характер  $\Omega$ ; 3, 4 принадлежит к  $Q$  (п. 263), вследствие чего ему в отрицательном собственно примитивном порядке соответствует род, все формы

которого имеют характеристическое число 1. Несобственно примитивного порядка в этом случае, так же, как и в следующем, не существует.

IV. Если  $M \equiv 2 \pmod{4}$ , то для того, чтобы из  $\Omega$  получился полный характер, к  $\Omega$  нужно добавить еще отношение к числу 8, а именно, либо 1 и 3, 8 либо 5 и 7, 8, если  $M \equiv 2 \pmod{8}$ , и либо 1 и 7, 8, либо 3 и 5, 8, если  $M \equiv 6 \pmod{8}$ . В первом случае характер  $\Omega$ ; 1 и 3, 8, очевидно, принадлежит к  $P$ , а потому характер  $\Omega$ ; 5 и 7, 8 — к  $Q$ , вследствие чего ему соответствует отрицательный собственно примитивный род; и по аналогичной причине во втором случае будет существовать *один* род из отрицательного собственно примитивного порядка, формы которого обладают требуемым свойством, именно, род с характером  $\Omega$ ; 3 и 5, 8.

Из этого следует, что отрицательные примитивные формы с определителем  $-M$ , имеющие характеристическое число 1, существуют, когда  $M$  сравнимо по модулю 8 с одним из чисел 1, 2, 3, 5, 6, причем всегда в одном единственном роде, который будет несобственным в случае  $M \equiv 3$ , и что таких форм вообще нет, если  $M \equiv 0, 4$  или  $7 \pmod{8}$ . Ясно также, что если  $(-a, -b, -c)$  является отрицательной примитивной формой с характеристическим числом  $+1$ , то  $(a, b, c)$  будет положительной примитивной формой с характеристическим числом  $-1$ . Отсюда видно, что в пяти первых случаях (когда  $M \equiv 1, 2, 3, 5, 6$ ) существует *один* положительный примитивный род, формы которого имеют характеристическое число  $-1$ , причем для  $M \equiv 3$  — несобственный, а в остальных трех случаях (когда  $M \equiv 0, 4, 7$ ) таких положительных форм вообще не может быть.

*Относительно собственных представлений двойничных форм тройничной формой  $x^2 + y^2 + z^2 = f$  из развитой в п. 282 общей теории получается следующее.*

I. Двойничная форма  $\varphi$  может быть собственно представлена формой  $f$  только если она (форма  $\varphi$ ) является положительной примитивной формой, и число  $-1$  (т. е. определитель формы  $f$ ) является ее характеристическим числом. Поэтому для положительных

определителей, а также и для отрицательных определителей —  $M$ , в случае когда  $M$  делится на 4 или имеет вид  $8n + 7$ , не существует двойничных форм, собственно представимых формой  $f$ .

II. Если же  $\varphi = (p, q, r)$  является положительной примитивной формой с определителем  $-M$ , и  $-1$  является характеристическим числом формы  $\varphi$ , а потому и противоположной ей формы  $(p, -q, r)$ , то существуют представления формы  $\varphi$  формой  $f$ , принадлежащие любому заданному значению выражения  $\sqrt{-(p, -q, r)}$ . Именно, все коэффициенты тройничной формы  $g$  с определителем  $-1$  (п. 283) обязательно будут целыми числами, а  $g$  будет определенной формой и потому заведомо будет эквивалентна форме  $f$  (п. 285, I).

III. Число всех принадлежащих одному и тому же значению выражения  $\sqrt{-(p, -q, r)}$  представлений во всех случаях, кроме случаев  $M = 1$  и  $M = 2$ , равно, согласно п. 283, III, числу преобразований формы  $f$  в  $g$ , и потому, согласно п. 285, равно 48; отсюда же вытекает, что если имеется *одно* принадлежащее заданному значению представление, то остальные 47 получатся, если значения  $x, y, z$  всевозможными способами переставлять и брать со всевозможными комбинациями знаков; поэтому все 48 представлений дают только одно разложение формы  $\varphi$  на три квадрата, если иметь в виду только сами квадраты, а не порядок их расположения и не знаки корней из них.

IV. Если количество всех входящих в  $M$  различных нечетных простых чисел положить равным  $\mu$ , то из п. 233 выводится, что число всех различных значений выражения  $\sqrt{-(p, -q, r)} \pmod{M}$  равно  $2^\mu$ , из которых, однако, согласно п. 283, нужно рассматривать только половину (если  $M > 2$ ). Поэтому число всех собственных представлений формы  $\varphi$  формой  $f$  равно  $48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+2}$ , а число различных разложений на три квадрата равно  $2^{\mu-1}$ .

**Пример.** Пусть  $\varphi = 19t^2 + 6tu + 41u^2$ , и потому  $M = 770$ . Здесь нужно рассматривать следующие четыре значения выражения  $\sqrt{-(19, -3, 4)} \pmod{770}$  (п. 283):  $(39, 237)$ ,  $(171, -27)$ ,  $(269, -83)$ ,  $(291, -127)$ . Чтобы найти представления, принадлежащие значению  $(39, 237)$ , мы сначала получаем тройничную форму  $\begin{pmatrix} 19, 41, 2 \\ 3, 6, 3 \end{pmatrix} = g$ ,

в которую, как мы находим по правилам из пп. 272, 275, форма  $f$  переходит при подстановке  $\begin{Bmatrix} 1, & -6, & 0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{Bmatrix}$ , откуда получается следующее представление формы  $\varphi$  формой  $f$ :

$$x = t - 6u, \quad y = -3t - 2u, \quad z = -3t - u;$$

остальные 47 представлений, принадлежащих этому же значению, которые получаются перестановками  $x, y, z$  и переменами знаков, мы ради краткости не выписываем. Все эти 48 представлений дают одно и то же разложение формы  $\varphi$  на три квадрата:

$$t^2 - 12tu + 36u^2, \quad 9t^2 + 12tu + 4u^2, \quad 9t^2 + 6tu + u^2.$$

Совершенно аналогичным образом значение  $(171, -27)$  дает разложение на квадраты  $(3t + 5u)^2, (3t - 4u)^2, t^2$ ; значение  $(269, -83)$  дает разложение  $(t + 6u)^2 + (3t + u)^2 + (3t - 2u)^2$ ; наконец, значение  $(291, -127)$  — разложение  $(t + 3u)^2 + (3t + 4u)^2 + (3t - 4u)^2$ ; каждое из этих разложений эквивалентно 48 представлениям. Кроме этих 192 представлений или четырех разложений, никаких других нет, так как 770 не делится ни на какой квадрат, и потому несобственных представлений существовать не может.

## 290

*Формы с определителями —1 и —2, которые в некоторых отношениях представляют собой исключения, мы коротко рассмотрим отдельно.* Сначала мы предположим общее замечание о том, что если  $\varphi, \varphi'$  какие-нибудь эквивалентные двойничные формы, и  $(\Theta)$  — заданное преобразование первой во вторую, то при комбинировании каждого представления формы  $\varphi$  некоторой тройничной формой  $f$  с подстановкой  $(\Theta)$  получается представление формой  $f$  формы  $\varphi'$ ; далее, при этом из собственных представлений формы  $\varphi$  получаются собственные представления форм  $\varphi'$ , причем из различных различные, а из всех — всевозможные такие представления формы  $\varphi'$ . Это очень легко можно доказать выкладкой. Поэтому

одна из форм  $\varphi$ ,  $\varphi'$  может быть представлена формой  $f$  столькими же способами, что и другая.

I. Пусть сначала  $\varphi = t^2 + u^2$  и  $\varphi'$  — какая-нибудь другая положительная двойничная форма с определителем  $-1$ , которой форма  $\varphi$  эквивалентна, и пусть  $\varphi$  переходит в  $\varphi'$  при подстановке  $t = \alpha t' + \beta u'$ ,  $u = \gamma t' + \delta u'$ . Форма  $\varphi$  представляется тройничной формой  $f = x^2 + y^2 + z^2$ , если положить  $x = t$ ,  $y = u$ ,  $z = 0$ ; при перестановках значений  $x$ ,  $y$ ,  $z$  отсюда получается шесть представлений, а из каждого из них — снова четыре, если изменять знаки у  $t$ ,  $u$ , так что всего имеется 24 представления, которым соответствует одно единственное разложение на три квадрата, и, кроме них, как легко видеть, никаких других быть не может. Отсюда следует, что и форма  $\varphi'$  может быть разложена на три квадрата только одним единственным способом, а именно, на  $(\alpha t' + \beta u')^2$ ,  $(\gamma t' + \delta u')^2$  и 0, каковому разложению эквивалентны 24 представления.

II. Пусть  $\varphi = t^2 + 2u^2$  и  $\varphi'$  — какая-нибудь другая положительная двойничная форма с определителем  $-2$ , и пусть  $\varphi$  переходит в нее при подстановке  $t = \alpha t' + \beta u'$ ,  $u = \gamma t' + \delta u'$ . Тогда, аналогично тому, как в предыдущем случае, мы заключаем, что  $\varphi$ , а потому и  $\varphi'$ , может быть разложена на три квадрата только одним единственным способом, а именно, форма  $\varphi$  — на  $t^2 + u^2 + u^2$  и форма  $\varphi'$  — на  $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$ ; легко видеть, что каждое такое разложение эквивалентно 24 представлениям.

Отсюда следует, что двойничные формы с определителями  $-1$  и  $-2$  относительно числа представлений тройничной формой  $x^2 + y^2 + z^2$  подчиняются закону, общему и для других двойничных форм; действительно, так как в обоих случаях  $\mu = 0$ , то формула предыдущего пункта также дает 24 представления. Причина этого заключается в том, что две особенности этих форм компенсируют одна другую.

Ради краткости мы освободим себя от труда применять к форме  $x^2 + y^2 + z^2$  изложенную в п. 284 общую теорию несобственных представлений.

Задача об отыскании всех собственных представлений заданного положительного числа  $M$  формой  $x^2 + y^2 + z^2$ , согласно п. 281, сводится сначала к отысканию собственных представлений числа  $-M$  формой  $-x^2 - y^2 - z^2 = f$ ; а это в соответствии с предписаниями п. 280 делается следующим образом.

I. Находятся все классы двойничных форм с определителем  $-M$ , формы которых могут быть собственно представлены формой  $X^2 + Y^2 + Z^2 = F$  (которая является дополнительной к форме  $f$ ). Если  $M \equiv 0, 4, 7 \pmod{8}$ , то, согласно п. 288, таких классов нет и потому  $M$  не может быть разложено на три квадрата, которые не имеют общих делителей\*. Если же  $M \equiv 1, 2, 5$ , или  $6$ , то существует один положительный собственно примитивный, или, если  $M \equiv 3$ , то несобственно примитивный род, который охватывает все такие классы; число этих классов мы обозначим через  $k$ .

II. Выберем теперь из этих классов любые  $k$  форм, из каждого класса по одной, которые мы обозначим через  $\varphi, \varphi', \varphi'', \dots$ , найдем всевозможные собственные представления этих форм формой  $F$ , число которых равно, таким образом  $3 \cdot 2^{\mu+3}k = K$ , где  $\mu$  обозначает количество (нечетных) простых сомножителей числа  $M$ , и выведем, наконец, из каждого такого представления

$$X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u$$

следующее представление формой  $x^2 + y^2 + z^2$  числа  $M$ :

$$x = m'n'' - m''n', \quad y = m''n - mn'', \quad z = mn' - m'n.$$

В совокупности этих  $K$  представлений, которую мы обозначим через  $\Omega$ , обязательно содержатся все представления числа  $M$ .

III. Поэтому нам нужно еще только исследовать, содержатся ли в  $\Omega$  одинаковые представления; а так как из п. 280, III мы уже знаем, что те представления из  $\Omega$ , которые получаются из различных

---

\* Это вытекает также и из того, что сумма трех нечетных квадратов обязательно  $\equiv 3 \pmod{8}$ , сумма двух нечетных и одного четного либо  $\equiv 2$ , либо  $\equiv 6$ , сумма одного нечетного и двух четных либо  $\equiv 1$ , либо  $\equiv 0$ , наконец, сумма трех четных либо  $\equiv 0$ , либо  $\equiv 4$ ; в последнем случае, однако, представление, очевидно, является несобственным.

форм, например, из форм  $\varphi$  и  $\varphi'$ , обязательно различны, то остается лишь исследовать, могут ли различные представления одной и той же формы, например, формы  $\varphi$ , формой  $F$  привести к одинаковым представлениям формой  $x^2 + y^2 + z^2$  числа  $M$ . Но тотчас же ясно, что если среди представлений формы  $\varphi$  имеется представление

$$(r) \quad X = mt + nu, \quad Y = m't + n'u, \quad Z = m''t + n''u,$$

то среди них есть и представление

$$(r') \quad X = -mt - nu, \quad Y = -m't - n'u, \quad Z = -m''t - n''u,$$

и что из обоих представлений получается одно и то же представление числа  $M$ , которое мы обозначим через  $(R)$ ; исследуем поэтому, может ли это представление  $(R)$  получиться еще из других представлений формы  $\varphi$ . Из п. 280, III легко следует, если положить  $X = \varphi$ , что если все собственные преобразования формы  $\varphi$  в себя представляются в виде

$$t = \alpha t + \beta u, \quad u = \gamma t + \delta u,$$

то все те представления формы  $\varphi$ , из которых следует представление  $(R)$ , выражаются формулами

$$\begin{aligned} x &= (\alpha m + \gamma n)t + (\beta m + \delta n)u, \\ y &= (\alpha m' + \gamma n')t + (\beta m' + \delta n')u, \\ z &= (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u. \end{aligned}$$

Но из изложенной в п. 179 теории преобразований двойничных форм с отрицательным определителем получается, что во всех случаях, кроме случаев  $M = 1$  и  $M = 3$ , имеется только два собственных преобразования формы  $\varphi$  в самое себя, именно,  $\alpha, \beta, \gamma, \delta$  (соответственно)  $= 1, 0, 0, 1$ , и  $= -1, 0, 0, -1$  (именно, так как  $\varphi$  является примитивной формой, то, что в п. 179 обозначалось через  $t$ , равно или 1 или 2, и потому всегда, кроме исключенных случаев, здесь заведомо имеет место случай 1 п. 179). Поэтому представление  $(R)$  может получиться только из представлений  $(r)$ ,  $(r')$ , и, значит, каждое собственное представление числа  $M$  встречается в  $\Omega$  два и только два раза, а количество всех различных собственных представлений числа  $M$  равно  $\frac{1}{2} K = 3 \cdot 2^{u+2k}$ .

Что касается исключенных случаев, то число собственных преобразований формы  $\varphi$  в себя, согласно п. 179, равно 4 для  $M = 1$  и равно 6 для  $M = 3$ , и, действительно, легко установить, что количества собственных представлений чисел 1, 3 равны соответственно  $K/4$ ,  $K/6$ ; именно, каждое из указанных двух чисел может быть разложено на три квадрата только одним единственным образом: число 1 — на  $1 + 0 + 0$ , число 3 — на  $1 + 1 + 1$ ; разложение числа 1 дает шесть, а разложение числа 3 — восемь различных представлений; число же  $K$  равно 24 для  $M = 1$  (когда  $\mu = 0$ ,  $k = 1$ ) и равно 48 для  $M = 3$  (когда  $\mu = 1$ ,  $k = 1$ ).

Кстати заметим, что если  $h$  равно числу классов в главном роде, которому, согласно п. 252, равно число классов в любом другом собственно примитивном роде, то  $k = h$  для  $M \equiv 1, 2, 5$  или  $6 \pmod{8}$ , и  $k = \frac{1}{3}h$  для  $M \equiv 3 \pmod{8}$ , за исключением единственного случая  $M = 3$ , когда  $k = h = 1$ . Поэтому для чисел вида  $8n + 3$  количество представлений всегда равно  $2^{\mu+2}h$ , так как для числа 3 две особенности компенсируют одна другую.

## 292

Разложения чисел на три квадрата мы различаем (так же, как и в случае двойничных форм) от представлений формой  $x^2 + y^2 + z^2$  в том отношении, что в первом случае мы обращаем внимание только на величину квадратов, а во втором, кроме того, на порядок их расположения и знаки квадратных корней из них, и потому представления  $x = a$ ,  $y = b$ ,  $z = c$  и  $x = a'$ ,  $y = b'$ ,  $z = c'$  мы считаем различными, если не выполняются одновременно равенства  $a = a'$ ,  $b = b'$ ,  $c = c'$ , в то время как разложения на  $a^2 + b^2 + c^2$  и  $a'^2 + b'^2 + c'^2$  считаются одинаковыми, если вторые квадраты с точностью до порядка расположения равны первым.

I. Из этого вытекает, что разложение числа  $M$  на квадраты  $a^2 + b^2 + c^2$  и  $a'^2 + b'^2 + c'^2$  эквивалентно 48 представлениям, если ни один из этих квадратов не равен 0 и все они различны между собой, и эквивалентно только 24 представлениям, если либо один из квадратов равен 0, а два других различны, либо ни один из квадратов не равен 0, но два из них одинаковы. Если же в разложении



заданного числа на три квадрата два из них равны 0, или один равен 0, а два других равны, или, наконец, все три равны между собой, то это разложение будет эквивалентно соответственно шести, двенадцати или восьми представлениям; однако, если ограничиваться только собственными представлениями, то так может быть только в исключительных случаях, когда  $M = 1$  или 2 или 3. Эти случаи мы из рассмотрения исключим и предположим, что количество всех разложений числа  $M$  на три квадрата (без общих делителей) равно  $E$ , и среди них имеется  $e$  разложений, в которых равен 0 один квадрат, и  $e'$  разложений, в которых два квадрата равны между собой; первые могут также рассматриваться как разложения на два квадрата, а вторые — на квадрат и удвоенный квадрат. Тогда количество всех собственных представлений числа  $M$  формой  $x^2 + y^2 + z^2$  равно

$$24(e + e') + 48(E - e - e') = 48E - 24(e + e').$$

Но из теории двойничных форм легко следует, что  $e$  равно либо 0, либо  $2^{\mu-1}$ , в зависимости от того, является ли число  $-1$  квадратичным невычетом или вычетом по модулю  $M$ , и точно так же  $e'$  равно либо 0, либо  $2^{\mu-1}$ , в зависимости от того, является невычетом или вычетом по модулю  $M$  число  $-2$ , где  $\mu$  равно количеству (нечетных) простых сомножителей числа  $M$  (см. п. 182; в большие] подробности мы здесь вдаваться не будем). Из этого легко выводится, что  $E = 2^{\mu-2}k$ , если как число  $-1$ , так и число  $-2$  являются невычетами по модулю  $M$ ,  $E = 2^{\mu-2}(k + 2)$ , если оба эти числа являются вычетами,  $E = 2^{\mu-2}(k + 1)$ , если одно число является вычетом, а другое невычетом по модулю  $M$ .

В исключительных случаях  $M = 1$  и  $M = 2$  эти формулы давали бы значение  $E = \frac{3}{4}$ , в то время как на самом деле  $E = 1$ ; для  $M = 3$  получается, однако, правильное значение  $E = 1$ , так как в этом случае две указанные в п. 291 особенности компенсируют одна другую.

Если поэтому  $M$  является простым числом, то  $\mu = 1$ , и потому  $E = \frac{1}{2}(k + 2)$ , в случае когда  $M \equiv 1 \pmod{8}$ ,  $E = \frac{1}{2}(k + 1)$ , когда  $M \equiv 3$  или  $\equiv 5$ . Эти частные теоремы были получены индуктивным

путем Лежандром и опубликованы им в замечательном, ранее уже упоминавшемся, сочинении, «*Hist. de l'Ac. de Paris*», 1785, р. 530 и след., правда, в несколько иной форме, причина чего в основном заключается в том, что он не различал собственную эквивалентность от несобственной и потому объединял между собой противоположные классы.

II. Чтобы найти все разложения числа  $M$  на три квадрата (без общих делителей) нет нужды находить все собственные представления всех форм  $\varphi, \varphi', \varphi'', \dots$ . Действительно, прежде всего легко установить, что все 48 представлений формы  $\varphi$ , которые принадлежат одному и тому же значению выражения  $\sqrt{-(p, -q, r)}$  (если положить  $\varphi = (p, q, r)$ ), дают одно и то же разложение числа  $M$ , и потому достаточно иметь только одно из них, или, что сводится к тому же, достаточно найти лишь все различные разложения\* формы  $\varphi$  на три квадрата, и точно так же обстоит дело для остальных форм  $\varphi', \varphi'', \dots$ . Далее, если  $\varphi$  не содержится в двустороннем классе, можно пренебречь формой, которая выбрана из противоположного класса, т. е. из каждой двух противоположных классов достаточно рассматривать только один. Действительно, так как совершенно безразлично, какая форма выбирается из каждого класса, то мы предположим, что из класса, противоположного тому, которому принадлежит форма  $\varphi$ , выбрана форма  $\varphi'$ , противоположная форме  $\varphi$ . Тогда легко видеть, что если собственные разложения формы  $\varphi$  в общем виде выражаются формулой

$$(gt + hu)^2 + (g't + h'u)^2 + (g''t + h''u)^2,$$

то все различные формы  $\varphi'$  будут представляться в виде

$$(gt - hu)^2 + (g't - h'u)^2 + (g''t - h''u)^2,$$

а также и то, что из последних получаются те же представления числа  $M$ , что и из первых. Наконец, в случае, когда  $\varphi$  является формой из двустороннего класса, но не формой главного класса и не формой, эквивалентной форме  $(2, 0, M/2)$  или форме  $(2, 1, (M+1)/2)$

---

\* Всегда нужно при этом подразумевать «собственные», если угодно перенести это выражение с представлений на разложения.

(в зависимости от того, четно  $M$  или нечетно), то половину значений выражения  $\sqrt{-(p, -q, r)}$  можно отбросить; ради краткости, однако, мы не будем говорить подробнее об этом преимуществе. Впрочем, если мы хотим получить все собственные представления числа  $M$  формой  $x^2 + y^2 + z^2$ , мы можем использовать это преимущество, так как оно легко получается из разложений.

Для примера найдем все разложения на три квадрата числа 770. Здесь  $\mu = 3$ ,  $e = e' = 0$  и потому  $E = 2k$ . В соответствии с классификацией положительных двойничных форм с определителем  $-770$ , которую мы здесь, ради краткости, приводить не будем, так как она легко может быть получена на основании любого из правил п. 231, мы находим, что число положительных классов равно 48, и все они собственно примитивны и распадаются на 8 родов, так что  $k = 4$ , и потому  $E = 8$ . Род, характеристическим числом которого является  $-1$ , должен, очевидно, иметь по отношению к числам 5, 7, 11 специальные характеры  $R5$ ;  $N7$ ;  $N11$ , из чего, на основании п. 263, легко следует, что его характер по отношению к числу 8 следующий: 1 и 3, 8. Но в роде, имеющем характер 1 и 3, 8;  $R5$ ;  $N7$ ;  $N11$ , имеется четыре класса, в качестве представителей которых мы выберем формы  $(6, 2, 129)$ ,  $(6, -2, 129)$ ,  $(19, 3, 41)$ ,  $(19, -3, 41)$ ; второй и четвертый классы мы, однако, отбросим, так как они противоположны соответственно первому и третьему классам. Четыре разложения формы  $(19, 3, 41)$  мы уже нашли в п. 289; из них получаются разложения числа 770 на  $9 + 361 + 400$ ,  $16 + 25 + 729$ ,  $81 + 400 + 289$ ,  $576 + 169 + 25$ . Подобным же образом находятся четыре разложения формы  $6t^2 + 4tu + 129u^2$  на

$$\begin{aligned} & t - 8u)^2 + (2t + u)^2 + (t + 8u)^2, \quad (t - 10u)^2 + (2t + 5u)^2 + (t + 2u)^2, \\ & (2t - 5u)^2 + (t + 10u)^2 + (t + 2u)^2, \quad (2t + 7u)^2 + (t - 8u)^2 + (t + 4u)^2, \end{aligned}$$

которые получаются соответственно из следующих значений выражения  $\sqrt{-(6, -2, 129)}$ :  $(48, 369)$ ,  $(62, -149)$ ,  $(92, -159)$ ,  $(202, 61)$ . Из этого вытекают разложения числа 770 на  $225 + 256 + 289$ ,  $1 + 144 + 625$ ,  $64 + 81 + 625$ ,  $16 + 225 + 529$ . Других разложений, кроме этих восьми, нет.

То, что относится к разложениям чисел на три квадрата, которые имеют общий делитель, настолько легко получается из общей теории п. 281, что нам нет нужды на этом останавливаться.

**Доказательство теоремы Ферма о том,  
что каждое целое число может быть разложено  
на три треугольных числа или на четыре квадрата**

293

Предыдущие исследования приводят также к доказательству знаменитой теоремы о том, что каждое положительное целое число может быть разложено на три треугольных числа, теоремы, которая впервые была найдена Ферма, но для которой до сих пор отсутствовало строгое доказательство. Очевидно, что каждое разложение числа  $M$  на треугольные числа

$$\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$$

дает возможность разложения числа  $8M+3$  на три нечетных квадрата

$$(2x+1)^2 + (2y+1)^2 + (2z+1)^2,$$

и обратно. Но, согласно изложенной выше теории, каждое целое положительное число  $8M+3$  разложимо на три квадрата, которые обязательно нечетны (ср. замечание к п. 291), и количество разложений зависит от количества простых сомножителей числа  $8M+3$  и от числа классов, на которые распадаются двойничные формы с определителем  $-(8M+3)$ . Столько же имеется и разложений числа  $M$  на три треугольных числа. При этом мы считаем, что  $x(x+1)/2$  рассматривается как треугольное число для любого значения  $x$ ; если же нуль желательно исключить, то теорему нужно формулировать так: каждое целое положительное число либо само является треугольным числом, либо разложимо на два или три треугольных числа. Подобное же изменение нужно будет внести и в следующую теорему, если будет желательно исключить нуль из числа рассматриваемых квадратов.

По такому же принципу доказывается и другая теорема Ф е р м а, а именно, что каждое целое положительное число может быть разложено на четыре квадрата. Если вычесть из числа вида  $4n + 2$  любой квадрат (который меньше, чем это число), из числа вида  $4n + 1$  — четный квадрат, или из числа вида  $4n + 3$  — нечетный квадрат, то во всех этих случаях остаток будет разложим на три квадрата, а потому исходное число — на четыре. Наконец, число вида  $4n$  может быть представлено как  $4^u N$ , где  $N$  имеет один из трех предыдущих видов; а если  $N$  разложимо на четыре квадрата, то тем самым будет разложимо и  $4^u N$ . От числа вида  $8n + 3$  можно вычесть также квадрат числа, делящегося на 4, от числа вида  $8n + 7$  — квадрат четного числа, не делящегося на 4, и от числа вида  $8n + 4$  — нечетный квадрат, причем остаток каждый раз будет разложим на три квадрата.

Впрочем, эта теорема была уже доказана Л а г р а н ж е м, «*Nouv. Mém. de l'Ac. de Berlin*», 1770, p. 123, причем это же доказательство (которое совершенно отлично от нашего) более подробно изложил Э й л е р в «*Actis Ac. Petz.*», vol. II, p. 48. Другие теоремы Ф е р м а, которые как бы образуют продолжение предыдущих, а именно, что каждое целое число разложимо на пять пятиугольных чисел, шесть шестиугольных, семь семиугольных и т. д., до сих пор не доказаны и требуют других методов.

### Решение уравнения $ax^2 + by^2 + cz^2 = 0$

294

Теорема. Если  $a$ ,  $b$ ,  $c$  обозначают взаимно простые числа, ни одно из которых не равно 0 и не делится ни на какой квадрат, то уравнение

$$(\Omega) \quad ax^2 + by^2 + cz^2 = 0$$

не имеет решений в целых числах (кроме решения  $x = y = z = 0$ , которое мы не принимаем во внимание), за исключением случая, когда числа  $-bc$ ,  $-ac$ ,  $-ab$  являются квадратичными вычетами соответственно по модулям  $a$ ,  $b$ ,  $c$ , и последние числа имеют различные

знаки; если же эти четыре условия выполняются, то уравнение  $(\Omega)$  в целых числах разрешимо.

**Доказательство.** Если уравнение  $(\Omega)$  вообще разрешимо в целых числах, то оно может быть удовлетворено также и такими значениями  $x, y, z$ , которые не имеют общих делителей; действительно, любые удовлетворяющие уравнению  $(\Omega)$  значения будут по-прежнему ему удовлетворять, если их разделить на их наибольший общий делитель. Если мы теперь предположим, что  $ap^2 + bq^2 + cr^2 = 0$ , и числа  $p, q, r$  свободны от общих делителей, то они будут также взаимно просты и попарно; в самом деле, если бы числа  $q, r$  имели общий делитель  $\mu$ , который был бы взаимно прост с  $p$ , то число  $\mu^2$  входило бы в  $ap^2$ , а значит, и в  $a$ , что противоречит предположению; точно так же взаимно просты одно с другим числа  $p, r$ ;  $p, q$ . Поэтому число  $-ap^2$  представляется двойничной формой  $by^2 + cz^2$ , когда  $y, z$  принимают взаимно простые значения  $q, r$ , вследствие чего определитель  $-bc$  этой формы является квадратичным вычетом по модулю  $ap^2$ , а значит, и по модулю  $a$  (п. 154). Точно так же имеет место  $-acRb$ ,  $-abRc$ . А тот факт, что уравнение  $(\Omega)$  не может иметь решений, если знаки чисел  $a, b, c$  одинаковы, настолько ясен, что не требует пояснений.

Доказательство обратного утверждения, составляющего вторую часть нашей теоремы, мы проведем так, что *сначала* покажем, как можно найти эквивалентную форме  $\begin{pmatrix} a & b & c \\ 0 & 0 & 0 \end{pmatrix} = f$  тройничную форму, у которой второй, третий, четвертый коэффициенты делятся соответственно на  $a, b, c$ , а из этого получим *затем* решение уравнения  $(\Omega)$ .

I. Найдем такие три числа  $A, B, C$ , которые не имеют общих делителей и обладают тем свойством, что  $A$  взаимно просто с числами  $b$  и  $c$ ,  $B$  взаимно просто с  $a$  и  $c$ ,  $C$  взаимно просто с  $a$  и  $b$ , и число  $aA^2 + bB^2 + cC^2$  делится на  $abc$ . Это достигается следующим образом. Пусть  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$  являются соответственно значениями выражений  $\sqrt{-bc} \pmod{a}$ ,  $\sqrt{-ac} \pmod{b}$ ,  $\sqrt{-ab} \pmod{c}$ , которые обязательно взаимно просты соответственно с числами  $a, b, c$ . Возьмем три целых числа  $\alpha, \beta, \gamma$ , которые взаимно просты соответственно с  $a, b, c$ , а в остальном совершенно произвольны

(например, все три равны 1) и определим  $A, B, C$  так, что

$$A \equiv bc \pmod{b} \text{ и } \equiv c\mathfrak{C} \pmod{c},$$

$$B \equiv ca \pmod{c} \text{ и } \equiv a\mathfrak{A} \pmod{a},$$

$$C \equiv ab \pmod{a} \text{ и } \equiv b\mathfrak{B} \pmod{b}.$$

Тогда

$$aA^2 + bB^2 + cC^2 \equiv a^2(b\mathfrak{A}^2 + cb^2) \equiv a^2(b\mathfrak{A}^2 - \mathfrak{A}^2b) \equiv 0 \pmod{a},$$

т. е. число  $aA^2 + bB^2 + cC^2$  делится на  $a$ , и точно так же делится на  $b$  и на  $c$ , а значит, и на произведение  $abc$ . Кроме того, получается, что  $A$  обязательно взаимно просто с  $b$  и  $c$ ,  $B$  взаимно просто с  $a$  и  $c$ ,  $C$  взаимно просто с  $a$  и  $b$ . Если эти же значения  $A, B, C$  имеют (наибольший) общий делитель  $\mu$ , то он, очевидно, будет взаимно прост с  $a, b, c$ , а потому и с  $abc$ ; поэтому если указанные значения разделить на  $\mu$ , то мы получим новые значения, которые не имеют общих делителей и при которых выражение  $aA^2 + bB^2 + cC^2$  все еще делится на  $abc$ , так что они удовлетворяют всем условиям.

II. Если числа  $A, B, C$  определены таким образом то не будут иметь общих делителей и числа  $Aa, Bb, Cc$ . Действительно, если бы они имели общий делитель  $\mu$ , то он обязательно должен был бы быть взаимно прост с  $a$  (так как  $a$  взаимно просто и с  $Bb$ , и с  $Cc$ ), и точно так же взаимно прост с  $b$  и с  $c$ ; поэтому  $\mu$  должно было бы входить в  $A, B, C$ , что противоречит предположению. Поэтому можно найти такие целые числа  $\alpha, \beta, \gamma$ , что  $\alpha Aa + \beta Bb + \gamma Cc = 1$ ; далее, найдем шесть таких чисел  $\alpha', \beta', \gamma', \alpha'', \beta'', \gamma''$ , что

$$\beta'\gamma'' - \beta''\gamma' = Aa, \quad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \quad \alpha'\beta'' - \beta'\alpha'' = Cc.$$

Если теперь  $f$  переходит при подстановке

$$\alpha, \alpha', \alpha'',$$

$$\beta, \beta', \beta'',$$

$$\gamma, \gamma', \gamma''$$

в форму  $\left(\begin{smallmatrix} m, m', m'' \\ n, n', n'' \end{smallmatrix}\right) = g$  (которая будет эквивалентна форме  $f$ ), то я утверждаю, что числа  $m', m'', n$  делятся на  $abc$ . Именно, если положить

$$\beta''\gamma - \gamma''\beta = A', \quad \gamma''\alpha - \alpha''\gamma = B', \quad \alpha''\beta - \beta''\alpha = C',$$

$$\beta\gamma' - \gamma\beta' = A'', \quad \gamma\alpha' - \alpha\gamma' = B'', \quad \alpha\beta' - \beta\alpha' = C'',$$

то будет иметь место

$$\begin{aligned}\alpha' &= B''C - C''B, & \beta' &= C''A - A''C, & \gamma' &= A''B - B''A, \\ \alpha'' &= C'B - B'C, & \beta'' &= A'C - C'A, & \gamma'' &= B'A - A'B.\end{aligned}$$

Если эти значения подставить в равенства

$$\begin{aligned}m' &= a\alpha'^2 + b\beta'^2 + c\gamma'^2, \\ m'' &= a\alpha''^2 + b\beta''^2 + c\gamma''^2, \\ n &= a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma'',\end{aligned}$$

то по модулю  $a$  получается

$$\begin{aligned}m' &\equiv bcA''^2 (B^2b + C^2c) \equiv 0, \\ m'' &\equiv bcA'^2 (B^2b + C^2c) \equiv 0, \\ n &\equiv bcA'A'' (B^2b + C^2c) \equiv 0,\end{aligned}$$

т. е. числа  $m'$ ,  $m''$ ,  $n$  делятся на  $a$ ; аналогичным же образом находят, что эти числа делятся также на  $b$ ,  $c$ , а потому и на  $abc$ .

III. Если мы положим для краткости определитель форм  $f$ ,  $g$ , т. е. число  $-abc$ , равным  $d$ , и

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N'',$$

то  $f$ , очевидно, будет переходить при подстановке (S)

$$\begin{array}{ccc}\alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma''\end{array}$$

в тройничную форму  $\begin{pmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{pmatrix} = g'$  с определителем  $d^3$ , которая, таким образом, содержится в  $f$ . Я утверждаю теперь, что форма  $\begin{pmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{pmatrix} = g''$  обязательно эквивалентна этой форме  $g'$ .

Действительно, очевидно, что  $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix} = g'''$  является тройничной формой с определителем 1; далее, так как, по предположению, числа  $a$ ,  $b$ ,  $c$  не все имеют одинаковые знаки, то  $f$  является неопределенной формой, откуда легко видеть, что должны быть неопределенными также и формы  $g'$  и  $g'''$ ; поэтому  $g'''$  эквивалентна



форме  $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$  (п. 277), и можно найти преобразование  $(S')$  первой формы во вторую; но очевидно, что этим преобразованием  $(S')$  форма  $g'$  будет переводиться в  $g''$ . Следовательно, также и  $g''$  содержится в  $f$ , и комбинация подстановок  $(S)$ ,  $(S')$  дает преобразование формы  $f$  в  $g''$ . Если этим преобразованием является

$$\begin{array}{ccc} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'', \end{array}$$

то ясно, что мы получаем два решения уравнения  $(\Omega)$ , а именно,  $x = \delta'$ ,  $y = \varepsilon'$ ,  $z = \zeta'$  и  $x = \delta''$ ,  $y = \varepsilon''$ ,  $z = \zeta''$ ; одновременно получается, что ни одна из этих двух систем значений не может быть нулевой, так как обязательно

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d.$$

**Пример.** Пусть задано уравнение  $7x^2 - 15y^2 + 23z^2 = 0$ ; оно разрешимо, так как  $345R7$ ,  $-161R15$ ,  $105R23$ . Для  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$  получаются значения 3, 7, 6, и если положить  $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$ , то мы находим  $A = 98$ ,  $B = -39$ ,  $C = -8$ . Отсюда выводится подста-

новка  $\begin{Bmatrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{Bmatrix}$ , которой форма  $f$  переводится в

$$\begin{pmatrix} 1520, & 14\,490, & -7245 \\ -2415, & -1\,246, & 4735 \end{pmatrix} = g. \text{ Поэтому}$$

$$(S) = \begin{Bmatrix} 7\,245, & 5, & 22 \\ -2\,415, & 2, & -28 \\ 19\,320, & 25, & -7 \end{Bmatrix}, \quad g''' = \begin{pmatrix} 3670800, & 6, & -3 \\ -1, & -1246, & 4735 \end{pmatrix}.$$

Далее мы находим, что форма  $g'''$  переходит в  $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$  при подстановке

$$(S') = \begin{Bmatrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{Bmatrix},$$

и если скомбинировать ее с (S), то получается подстановка

$$\begin{pmatrix} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3 \end{pmatrix},$$

при которой  $f$  переходит в  $g''$ . Мы получаем поэтому два решения заданного уравнения:  $x = 11, y = 9, z = 4$  и  $x = 12, y = -9, z = 3$ . Последнее решение сделается проще, если поделить значения на общий делитель 3, после чего получится  $x = 4, y = -3, z = 1$ .

295

Последняя часть теоремы предыдущего пункта может быть также получена и следующим образом. Найдем целое число  $h$  с тем свойством, что  $ah \equiv \mathfrak{C} \pmod{c}$  (буквы  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$  мы употребляем в том же значении, что и в предыдущем пункте), и положим  $ah^2 + b = ci$ . Тогда легко видеть, что  $i$  — целое число, и  $-ab$  является определителем двойничной формы  $(ac, ah, i) = \varphi$ . Эта форма заведомо не положительна (действительно, так как, по предположению,  $a, b, c$  не все имеют одинаковые знаки, числа  $ab$  и  $ac$  не могут одновременно быть положительными); далее, она имеет характеристическое число  $-1$ , что мы докажем следующим образом. Если определить целые числа  $e, e'$  так, что  $e \equiv 0 \pmod{a}$  и  $\equiv \mathfrak{B} \pmod{b}$ ,  $ce' \equiv \mathfrak{A} \pmod{a}$  и  $h\mathfrak{B} \pmod{b}$ , то  $(e, e')$  будет значением выражения  $\sqrt{-(ac, ah, i)} \pmod{-ab}$ . Действительно, по модулю  $a$  имеет место

$$\begin{aligned} e^2 &\equiv 0 \equiv -ac, & ee' &\equiv 0 \equiv -ah, \\ c^2 e'^2 &\equiv \mathfrak{A}^2 \equiv -bc \equiv -c^2 i, & \text{и потому} & e'^2 \equiv -i; \end{aligned}$$

а по модулю  $b$ :

$$\begin{aligned} e^2 &\equiv \mathfrak{B}^2 \equiv -ac, & cee' &\equiv h\mathfrak{B}^2 \equiv -ach, & \text{и потому} & ee' \equiv -ah, \\ c^2 e'^2 &\equiv h^2 \mathfrak{B}^2 \equiv -ach^2 \equiv -c^2 i, & \text{и потому} & e'^2 \equiv -i. \end{aligned}$$

Но эти же три сравнения, которые выполняются по каждому из модулей  $a, b$ , справедливы и по модулю  $ab$ . Из этого на основании теории тройничных форм легко видеть, что  $\varphi$  представима формой  $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ . Пусть, таким образом,

$$act^2 + 2ahtu + iu^2 \equiv -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u);$$

тогда, если умножить это равенство на  $c$ , получается

$$a(ct + hu)^2 + bu^2 = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u).$$

Отсюда вытекает, что если придать  $t, u$  такие значения, что либо  $\gamma t + \delta u = 0$ , либо  $\varepsilon t + \zeta u = 0$ , то мы тем самым получим решение уравнения  $(\Omega)$ , которое, следовательно, будет удовлетворяться как значениями

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha \delta - \beta \gamma,$$

так и значениями

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha \zeta - \beta \varepsilon.$$

Кроме того, ясно, что как первые, так и вторые значения не могут быть одновременно все равны 0; действительно, если бы было  $\delta c - \gamma h = 0$  и  $\gamma = 0$ , то имело бы место также  $\delta = 0$  и  $\varphi = -(\alpha t + \beta u)^2$ , откуда  $ab = 0$ , что противоречит предположению, и так же обстоит дело в отношении других значений. В нашем примере в качестве  $\varphi$  мы находим форму (161, — 63, 24), в качестве значения выражения  $\sqrt{-\varphi} \pmod{105}$  — значение (7, — 51), и в качестве представления формы  $\varphi$  формой  $\begin{pmatrix} -1, & 0, & 0 \\ & 1, & 0, & 0 \end{pmatrix}$  — представление

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u).$$

откуда получаются решения  $x = 7, \quad y = 11, \quad z = -8; \quad x = 20, \quad y = 15, \quad z = -5$ , или, если последнее решение разделить на 5 и отбросить знак у  $z$ ,  $x = 4, \quad y = 3, \quad z = 1$ .

Из этих двух методов решения уравнения  $(\Omega)$  последний имеет то преимущество, что он в большинстве случаев имеет дело с меньшими числами; однако первый, который может быть также соединен с различными искусственными приемами, на которых мы здесь не останавливались, представляется более изящным, особенно по той причине, что числа  $a, b, c$  рассматриваются здесь как равноправные, и при перестановке их выкладки совершенно не меняются. Во втором случае дело обстоит по-иному, так как здесь вычисления по большей части удобнее всего производить, если принимать за  $a$  наименьшее, а за  $c$  наибольшее из трех заданных чисел, как мы и делали в нашем примере.

## О методе, которым Лежандр изложил фундаментальную теорему \*

296

Изящная теорема, изложенная в предыдущих пунктах, впервые была найдена и подкреплена красивым доказательством (совершенно отличным от обоих наших доказательств) Лежандром, «*Hist. de Ac. de Paris*», 1785, p. 507. Однако одновременно этот замечательный математик попытался в указанном месте вывести доказательство теоремы, которая совпадает с фундаментальной теоремой предыдущего раздела, из того, что, как мы уже поясняли выше (п. 151), на наш взгляд, не совсем пригодно для этой цели. Поэтому будет уместным кратко изложить здесь это (само по себе в высшей степени изящное) доказательство и указать на причину такого нашего мнения. Сначала предпосылается следующее замечание.

Если числа  $a, b, c$  все  $\equiv 1 \pmod{4}$ , то уравнение

$$(\Omega) \quad ax^2 + by^2 + cz^2 = 0$$

не разрешимо. Действительно, легко видеть, что значение выражения  $ax^2 + by^2 + cz^2$  в этом случае обязательно будет либо  $\equiv 1$ , либо  $\equiv 2$ , либо  $\equiv 3 \pmod{4}$ , если считать, что не все величины  $x, y, z$  одновременно четны. Если бы поэтому уравнение  $(\Omega)$  было разрешимо, то это могло бы достигаться только при четных значениях  $x, y, z$ , что является абсурдом, так как любые значения, удовлетворяющие уравнению  $(\Omega)$ , будут по-прежнему ему удовлетворять, если их разделить на их наибольший общий делитель, после чего хотя бы одно из них обязательно сделается нечетным. Теперь различные случаи доказываемой теоремы сводятся к следующим основным моментам.

I. Если  $p, q$  обозначают (положительные различные) простые числа вида  $4n + 3$ , то не может одновременно иметь место  $pRq$  и  $qRp$ . Действительно, если бы это было возможно, если положить  $1 = a, -p = b, -q = c$ , выполнялись бы все условия, необходимые для разрешимости уравнения  $ax^2 + by^2 + cz^2 = 0$  (п. 294); однако оно, согласно предпосланному замечанию, решений не

---

\* Ср. дополнения в конце «Исследований».

имеет; следовательно, предположение не может быть верным. Отсюда тотчас же вытекает теорема 7 из п. 131.

II. Если  $p$  является простым числом вида  $4n + 1$ , а  $q$  — простым числом вида  $4n + 3$ , то не может одновременно иметь места  $qRp$ ,  $pNq$ . Действительно, в противном случае было бы  $-pRq$ , и уравнение  $x^2 + py^2 - qz^2 = 0$  имело бы решение, что согласно предпосланному замечанию, невозможно. Отсюда получаются случаи 4 и 5 из п. 131.

III. Если  $p$ ,  $q$  являются простыми числами вида  $4n + 1$ , то не может одновременно иметь места  $pRq$  и  $qNp$ . Возьмем некоторое простое число  $r$  вида  $4n + 3$ , которое является вычетом по модулю  $q$  и по которому  $p$  есть невычет. Тогда, согласно доказанным выше (II) случаям имеет место  $qRr$ ,  $qNp$ . Если бы поэтому было  $pRq$ ,  $qNp$ , то имело бы место  $qrRp$ ,  $prRq$ ,  $pqNr$ , и потому  $-pqRr$ . Следовательно, вопреки предпосланному замечанию, уравнение  $px^2 + qy^2 - rz^2 = 0$  было бы разрешимо; поэтому сделанное предположение не может выполняться. Отсюда получаются случаи 1 и 2 из п. 131.

Короче этот случай излагается следующим образом. Если  $r$  обозначает простое число вида  $4n + 3$ , по которому  $p$  является невычетом, то также  $rNp$ , и потому (если предположить, что  $pRq$ ,  $qNp$ )  $qrRp$ ; далее,  $-pRq$ ,  $-pRr$ , и тем самым также  $-pRqr$ ; поэтому уравнение  $x^2 + py^2 - qrz^2 = 0$  было бы разрешимо, что противоречит предпосланному замечанию. Следовательно, и т. д.

IV. Если  $p$  является простым числом вида  $4n + 1$ , а  $q$  — простым числом вида  $4n + 3$ , то не может быть одновременно  $pRq$  и  $qNp$ . Возьмем вспомогательное простое число  $r$  вида  $4n + 1$ , которое является невычетом по каждому из чисел  $p$ ,  $q$ . Тогда (согласно II) имеет место  $qNr$ , и (согласно III)  $pNr$ ; отсюда  $pqRr$ . Если поэтому было бы  $pRq$ ,  $qNp$ , то мы имели бы также  $prNq$ ,  $-prRq$ ,  $qrRp$ ; тем самым уравнение  $px^2 - qy^2 + rz^2 = 0$  было бы разрешимо, что невозможно. Отсюда получаются случаи 3 и 6 из п. 131.

V. Если  $p$ ,  $q$  обозначают простые числа вида  $4n + 3$ , то не может одновременно быть  $pNq$  и  $qNp$ . Действительно, если мы предположим, что это возможно, и возьмем вспомогательное простое число  $r$  вида  $4n + 1$ , которое является невычетом по каждому из чисел

$p, q$ , то будет иметь место  $qrRp, prRq$ ; далее, согласно II,  $pNr, qNr$ , и потому  $pqRr$  и  $-pqRr$ . Следовательно, уравнение  $-px^2 - qy^2 + + rz^2 = 0$  было бы разрешимо, что находится в противоречии с предпосланным замечанием. Отсюда следует случай 8 из п. 131.

## 297

Рассматривая предыдущее доказательство подробнее, легко убедиться, что случаи I и II разобраны так, что против них возразить нечего. Однако доказательства остальных случаев опираются на некоторые леммы, и если они еще не доказаны, то и весь метод, очевидно, теряет свое значение. Хотя эти предположения таковы, что при поверхностном рассмотрении могло бы показаться, что они и не требуют доказательства вследствие своей совершенной *очевидности*, все же они не могут быть приняты на веру, если желать полной математической строгости. Что касается предположения в IV и V о том, что существует простое число  $r$  вида  $4n + 1$ , которое является невычетом по двум другим заданным простым числам  $p, q$ , то из четвертого раздела легко следует, что все числа, которые меньше чем  $4pq$  и взаимно просты с этим числом (количество их равно  $2(p - 1)(q - 1)$ ), равномерно распределяются по четырем классам, один из которых содержит невычеты по каждому из чисел  $p, q$ , а три остальных содержат вычеты по модулю  $p$  и невычеты по модулю  $q$ , невычеты по модулю  $p$  и вычеты по модулю  $q$ , и, наконец, вычеты по обоим модулям  $p, q$ , и что в отдельных классах половина чисел имеет вид  $4n + 1$ , а половина — вид  $4n + 3$ . Поэтому среди всех этих чисел имеется  $(p - 1)(q - 1)/4$  невычетов вида  $4n + 1$  по каждому из модулей  $p, q$ ; эти невычеты мы обозначим через  $g, g', g'', \dots$ , а остальные  $7(p - 1)(q - 1)/4$  чисел — через  $h, h', h'', \dots$ . Очевидно, что все числа вида  $4pqt + g, 4pqt + g', 4pqt + + g'', \dots$  тоже будут иметь вид  $4n + 1$  и будут невычетами по модулям  $p, q$ ; совокупность этих чисел обозначим через  $(G)$ . Теперь ясно, что для обоснования предположения нужно только доказать, что в совокупности  $(G)$  заведомо содержатся простые числа; само по себе это очень вероятно, так как формы из  $(G)$  вместе с формами  $4pqt + h, 4pqt + h', \dots$ , совокупность которых мы обозначим через

( $H$ ), содержат все числа, взаимно простые с  $4pq$ , а потому и все простые числа (кроме чисел  $2, p, q$ ), и не видно причин, по которым ряд простых чисел не распределялся бы по этим формам равномерно, так что восьмая их часть принадлежит к ( $G$ ), а остальные к ( $H$ ). Однако ясно, что такой вывод лишен математической строгости. Л е ж а н д р сам замечает, что доказательство теоремы о том, что в каждой форме вида  $kt + l$ , где  $k, l$  обозначают заданные взаимно простые числа, а  $t$  — произвольное число, обязательно содержатся простые числа, оказывается довольно трудным, и вскользь указывает метод, который, быть может, способен привести к этому доказательству. Однако, как нам кажется, для того, чтобы получить на этом пути строгое доказательство, нужны многие подготовительные исследования.

Относительно другого предположения (III, второй метод), а именно, что имеется простое число  $r$  вида  $4n + 3$ , по которому другое заданное простое число  $p$  вида  $4n + 1$  является невычетом, Л е ж а н д р вообще не добавляет никакого замечания. Выше (п. 129) мы доказали, что заведомо существуют простые числа, по которым  $p$  является невычетом, но аш метод оказывается недостаточным, чтобы доказать существование таких простых чисел, которые одновременно имеют вид  $4n + 3$  (что не требовалось в нашем первом доказательстве, но требуется здесь). Впрочем, справедливость этого предположения мы легко можем доказать следующим образом. Согласно п. 287, существует положительный род двойничных форм с определителем  $-p$ , имеющий характер  $3, 4; Nr$ ; пусть  $(a, b, c)$  — такая форма, и  $a$  нечетно (что мы имеем право предполагать). Тогда  $a$  имеет вид  $4n + 3$  и либо само будет простым числом, либо будет делиться по крайней мере на одно простое число  $r$  вида  $4n + 3$ . Но  $-pRa$ , и потому также  $-pRr$ , а, значит,  $pNr$ . Однако, нужно заметить, что теоремы пп. 263, 287 опираются на фундаментальную теорему, и потому, если бы мы захотели доказывать на основании их часть фундаментальной теоремы, получился бы порочный круг. Наконец, предположение первого метода из III еще более произвольно, так что нет нужды добавлять о нем что-либо еще.

Быть может, стоит добавить еще одно замечание относительно случая V, который хотя и не доказан изложенным только что ме-

тодом, но легко может быть закончен следующим образом. Если бы там одновременно имело место  $pNq$ ,  $qNr$ , то было бы  $-pRq$ ,  $-qRp$ , откуда легко видеть, что  $-1$  является характеристическим числом формы  $(p, 0, q)$ , которая тем самым (согласно теории тройных форм) может быть представлена формой  $x^2 + y^2 + z^2$ . Если

$$pt^2 + qu^2 = (\alpha t + \beta u)^2 + (\alpha' t + \beta' u)^2 + (\alpha'' t + \beta'' u)^2,$$

или

$$\alpha^2 + \alpha'^2 + \alpha''^2 = p, \quad \beta^2 + \beta'^2 + \beta''^2 = q, \quad \alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0,$$

то вследствие первого и второго равенств все числа  $\alpha$ ,  $\alpha'$ ,  $\alpha''$ ,  $\beta$ ,  $\beta'$ ,  $\beta''$  будут нечетны. Но тогда, очевидно, не может выполняться третье равенство. Подобным же образом может быть рассмотрен и случай II.

298

**Задача.** Пусть  $a$ ,  $b$ ,  $c$  обозначают любые числа; найти условия для разрешимости уравнения

$$(\omega) \quad ax^2 + by^2 + cz^2 = 0.$$

**Решение.** Пусть  $\alpha^2$ ,  $\beta^2$ ,  $\gamma^2$  обозначают наибольшие квадраты, входящие соответственно в числа  $bc$ ,  $ac$ ,  $ab$ , и пусть  $\alpha a = \beta \gamma A$ ,  $\beta b = \alpha \gamma B$ ,  $\gamma c = \alpha \beta C$ . Тогда  $A$ ,  $B$ ,  $C$  являются целыми взаимно простыми числами; уравнение же  $(\omega)$  будет разрешимо или нет, в зависимости от того, имеет или нет решение уравнение

$$(\Omega) \quad AX^2 + BY^2 + CZ^2 = 0,$$

что можно узнать на основании п.294.

**Доказательство.** Если положить  $bc = \mathfrak{A}\alpha^2$ ,  $ac = \mathfrak{B}\beta^2$ ,  $ab = \mathfrak{C}\gamma^2$ , то  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$  будут целыми числами, свободными от квадратных сомножителей, и будет иметь место  $\mathfrak{A} = BC$ ,  $\mathfrak{B} = AC$ ,  $\mathfrak{C} = AB$ . Следовательно,  $\mathfrak{A}\mathfrak{B}\mathfrak{C} = (ABC)^2$ , и потому число  $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$  обязательно будет целым. Если  $m$  является наибольшим общим делителем чисел  $\mathfrak{A}$ ,  $A\mathfrak{A}$  и  $\mathfrak{A} = gt$ ,  $A\mathfrak{A} = ht$ , то  $g$  взаимно просто с  $h$ , а также и с  $m$  (ибо  $\mathfrak{A}$  не имеет квадратных сомножителей)



Теперь  $h^2m = gA^2\mathfrak{A} + g\mathfrak{B}\mathfrak{C}$ , и потому  $g$  входит в  $h^2m$ , что, очевидно, невозможно, если  $g$  не равно  $\pm 1$ . Поэтому  $\mathfrak{A} = \pm m$ ,  $A = \pm h$ ; тем самым  $A$  является целым числом, и точно так же целыми будут и числа  $B$  и  $C$ . Так как  $\mathfrak{A} = BC$  не имеет квадратных делителей, то  $B$  и  $C$  обязательно должны быть взаимно просты. Наконец, ясно, что если уравнение  $(\Omega)$  удовлетворяется при значениях  $X = P$ ,  $Y = Q$ ,  $Z = R$ , уравнению  $(\omega)$  будут удовлетворять значения  $x = \alpha P$ ,  $y = \beta Q$ ,  $z = \gamma R$ , и наоборот, если второе уравнение удовлетворяется при значениях  $x = p$ ,  $y = q$ ,  $z = r$ , то значения  $X = \beta\gamma p$ ,  $Y = \alpha\gamma q$ ,  $Z = \alpha\beta r$  будут решениями первого, так что либо оба эти уравнения разрешимы, либо не разрешимо ни то, ни другое.

### Представление нуля любыми тройничными формами

299

**Задача.** Пусть дана тройничная форма

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx';$$

определить, может ли быть представлен этой формой нуль (при значениях неизвестных, которые не все равны 0).

**Решение.** I. Если  $a = 0$ , то значения неизвестных  $x'$ ,  $x''$  могут быть взяты произвольно, а из уравнения

$$a'x'^2 + 2bx'x'' + a''x''^2 = -2x(b'x'' + b''x')$$

вытекает тогда, что  $x$  получает определенное рациональное значение; если при этом для  $x$  получается дробное значение, то нужно только умножить значения  $x$ ,  $x'$ ,  $x''$  на знаменатель этой дроби, после чего получатся целые числа. Невозможными для  $x'$ ,  $x''$  являются те и только те значения, для которых  $b'x'' + b''x' = 0$ , причем не имеет место одновременно  $a'x'^2 + 2bx'x'' + a''x''^2 = 0$ , когда  $x$  можно взять произвольным. Одновременно ясно, что таким путем можно получить все возможные решения. Случай, когда  $b' = b'' = 0$ , можно не рассматривать; действительно, тогда  $x$  совсем не входит в  $f$ , т. е.  $f$  является двойничной формой, и о представимости нуля формой  $f$  нужно судить на основании теории таких форм.

II. Если же  $a$  не равно 0, то уравнение  $f = 0$  эквивалентно уравнению

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = 0,$$

если положить

$$b''^2 - aa' = A'', \quad ab - b'b'' = B, \quad b'^2 - aa'' = A'.$$

Если теперь здесь  $A'' = 0$ , но  $B$  не равно 0, то очевидно, что если взять произвольными значения  $ax + b''x' + b'x''$  и  $x''$ , то  $x$  и  $x'$  определятся рациональным образом, и в случае, когда они не будут целыми числами, можно будет найти подходящий множитель, который приведет к целым значениям. Лишь для одного единственного значения  $x''$ , именно, для  $x'' = 0$ , значение  $ax + b''x + b'x''$  не произвольно, а тоже должно быть равным 0; но тогда можно брать произвольно значения  $x'$ , и для  $x$  будет получаться рациональное значение. Если же одновременно  $A'' = 0$  и  $B = 0$ , то ясно, что если  $A'$  равно некоторому квадрату  $k^2$ , то уравнение  $f = 0$  сводится к следующим двум линейным уравнениям (из которых должно удовлетворяться либо одно, либо другое):

$$ax + b''x' + (b' + k)x'' = 0, \quad ax + b''x' + (b' - k)x'' = 0;$$

если же (при том же предположении)  $A'$  не является квадратом, то очевидно, что решение заданного уравнения равносильно решению уравнений  $x'' = 0$  и  $ax + b''x' = 0$  (которые должны удовлетворяться одновременно).

Едва ли нужно указывать, что метод из I может применяться также и тогда, когда равно нулю  $a'$  или  $a''$ , а метод из II, — когда  $A' = 0$ .

III. Если же ни  $a$ , ни  $A''$  не равно 0, то уравнение  $f = 0$  эквивалентно следующему:

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Da x''^2 = 0,$$

где через  $D$  обозначен определитель формы  $f$ , т. е. через  $Da$  — число  $B^2 - A'A''$ . Если  $D = 0$ , то в отношении решения дело обстоит аналогично тому, как в конце предыдущего случая; именно,

если  $A''$  является квадратом, причем равно  $k^2$ , то заданное уравнение сводится к следующим:

$$\begin{aligned} kax + (kb'' - A'')x' + (kb' + B)x'' &= 0, \\ kax + (kb'' + A'')x' + (kb' - B)x'' &= 0; \end{aligned}$$

если же  $A''$  не является квадратом, то нужно положить

$$ax + b''x' + b'x'' = 0, \quad A''x' - Bx'' = 0.$$

Если, напротив,  $D$  не равно нулю, то мы приходим к уравнению

$$A''t^2 - u^2 + Dav^2 = 0.$$

о разрешимости которого мы можем судить на основании предыдущего пункта. Если теперь последнее уравнение не может быть решено иначе, как посредством значений  $t = 0$ ,  $u = 0$ ,  $v = 0$ , то и заданное уравнение, очевидно, не будет обладать другими решениями, кроме  $x = 0$ ,  $x' = 0$ ,  $x'' = 0$ ; если же уравнение  $A''t^2 - u^2 + Dav^2 = 0$  разрешимо еще каким-нибудь образом, то из любых значений  $t$ ,  $u$ ,  $v$  на основании уравнений

$$ax + b''x' + b'x'' = t, \quad A''x' - Bx'' = u, \quad x'' = v$$

получаются, вообще говоря, рациональные значения  $x$ ,  $x'$ ,  $x''$ , из которых, если они содержат дроби, при помощи подходящего множителя можно получить целые значения.

Но если найдено какое-нибудь одно решение уравнения  $f = 0$  в целых числах, то задача может быть сведена к случаю I, и так же, как и там, могут быть найдены все решения. Это достигается следующим образом.

Пусть уравнению  $f = 0$  удовлетворяют значения (которые мы предполагаем свободными от общих делителей)  $\alpha$ ,  $\alpha'$ ,  $\alpha''$  неизвестных  $x$ ,  $x'$ ,  $x''$ ; выберем, далее (в соответствии с пп. 40 и 279), такие целые числа  $\beta$ ,  $\beta'$ ,  $\beta''$ ,  $\gamma$ ,  $\gamma'$ ,  $\gamma''$ , что

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1,$$

(и пусть  $f$  при подстановке

S)  $x = \alpha y + \beta y' + \gamma y''$ ,  $x' = \alpha' y + \beta' y' + \gamma' y''$ ,  $x'' = \alpha'' y + \beta'' y' + \gamma'' y''$  переходит в форму

$$g = cy^2 + c'y'^2 + c''y''^2 + 2dy'y'' + 2d'y''y + 2d''yy'.$$

Тогда, очевидно,  $c = 0$  и  $g$  будет эквивалентна форме  $f$ , откуда легко следует, что из всех решений уравнения  $g = 0$  получаются (при помощи подстановки  $(S)$ ) все целочисленные решения уравнения  $f = 0$ . Но из I следует, что все решения уравнения  $g = 0$  содержатся в формулах

$y = -z(c'p^2 + 2dpq + c''q^2)$ ,  $y' = 2z(d''p^2 + d'pq)$ ,  $y'' = 2z(d''pq + d'q^2)$ , где  $p, q$  обозначают произвольные целые числа, а  $z$  — произвольное число, для которого можно брать и дробные значения, если только  $y, y', y''$  остаются при этом целыми числами. Если подставлять эти значения  $y, y', y''$  в  $(S)$ , то мы получим всевозможные целочисленные решения уравнения  $f = 0$ .

Так, например, если дана форма

$$f = x^2 + x'^2 + x''^2 - 4x'x'' + 2xx'' + 8xx'$$

и дано *одно* решение  $x = 1, x' = -2, x'' = 1$  уравнения  $f = 0$ , то, полагая  $\beta, \beta', \beta'', \gamma, \gamma', \gamma''$  равными соответственно  $0, 1, 0, 0, 0, 1$ , мы получаем, что

$$g = y'^2 + y''^2 - 4y'y'' + 12yy''.$$

Все целочисленные решения уравнения  $g = 0$  содержатся в формулах

$$y = -z(p^2 - 4pq + q^2), \quad y' = 12zpq, \quad y'' = 12zq^2,$$

и потому все решения уравнения  $f = 0$  — в формулах

$$\begin{aligned} x &= -z(p^2 - 4pq + q^2), \\ x' &= 2z(p^2 + 2pq + q^2), \\ x'' &= -z(p^2 - 4pq - 11q^2). \end{aligned}$$

**Общее решение в рациональных величинах  
уравнений второй степени с двумя неизвестными**

Из решения задачи предыдущего пункта сразу получается также решение неопределенного уравнения

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0,$$

когда требуется найти рациональные значения; решение этого же уравнения в целых числах уже было изложено выше (п. 216 и сл.). Действительно, все рациональные значения неизвестных  $x, y$  могут быть представлены в виде  $t/v, u/v$ , где  $t, u, v$  — целые числа, откуда вытекает, что решение этого уравнения в рациональных числах равносильно решению уравнения

$$at^2 + 2btu + cu^2 + 2dtv + 2euv + fv^2 = 0$$

в целых числах; а это уравнение совпадает с рассмотренным в предыдущем пункте. Должны быть исключены лишь те решения, где  $v = 0$ ; однако их не может быть, если число  $b^2 - ac$  не является квадратом. Так, например, все решения в рациональных числах уравнения

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$$

(решенного в п. 221 в целых числах) содержатся в формулах

$$x = \frac{p^2 - 4pq + q^2}{p^2 - 4pq - 11q^2}, \quad y = -\frac{2p^2 + 4pq + 2q^2}{p^2 - 4pq - 11q^2},$$

где  $p, q$  обозначают произвольные целые числа. Впрочем, мы здесь лишь кратко коснулись обеих этих находящихся в теснейшей взаимной связи задач и опустили многие относящиеся сюда замечания, чтобы не быть слишком пространными, с одной стороны, а с другой, — потому что мы владеем другим, основанным на более общих принципах, решением задачи предыдущего пункта, изложение которого мы должны оставить до другого случая, так как оно требует более подробного исследования тройничных форм.

### О среднем количестве родов

#### 301

*Мы возвращаемся к двойничным формам, многие особые свойства которых мы еще должны привести. Сначала мы добавим некоторые замечания относительно числа родов и классов в собственно примитивном (для отрицательного определителя положительном) порядке, которым мы ограничимся ради краткости.*

Число родов, на которые распадаются все (собственно примитивные положительные) формы с заданным положительным или отрицательным определителем  $\pm D$  всегда равно 1, 2, 4 или более высокой степени числа 2, показатель которой зависит от сомножителей числа  $D$  и на основании предыдущих исследований может быть определен *a priori*. Но так как в ряду натуральных чисел простые числа перемешаны с составными, имеющими то большее, то меньшее количество делителей, то оказывается, что для нескольких следующих один за другим определителей  $\pm D, \pm (D + 1), \pm (D + 2), \dots$  число родов то возрастает, то убывает, и в этой запутанной последовательности не видно никакой закономерности. Тем не менее, если сложить количества родов, которые соответствуют многим, следующим один за другим определителям

$$\pm D, \quad \pm (D + 1), \dots, \quad \pm (D + m),$$

и сумму поделить на количество этих определителей, то получится *среднее число родов*, которое может рассматриваться как соответствующее среднему значению  $\pm (D + \frac{1}{2}m)$  определителей и которое образует очень правильный ряд. Мы будем, однако, предполагать, что не только  $m$  достаточно велико, но что и  $D$  еще на много больше, чтобы отношение крайних определителей не слишком отличалось от единицы. Закономерность указанного ряда нужно понимать следующим образом. Если число  $D'$  во много раз больше, чем  $D$ , то и среднее число родов, соответствующее определителю  $\pm D'$ , будет значительно больше, чем для определителя  $D$ ; если же  $D$  и  $D'$  мало отличаются друг от друга, то и среднее число родов по отношению к  $D$  и  $D'$  будет почти одинаково. При этом среднее число родов по отношению к положительному определителю  $+D$  всегда приблизительно равно среднему числу родов по отношению к отрицательному определителю  $-D$ , причем тем точнее, чем больше  $D$ , в то время как для маленького значения  $D$  первое немного больше, чем второе. Эти замечания сделаются яснее благодаря следующим примерам, которые мы почерпнули из таблицы разбиения двойничных форм на классы, охватывающей более 4000 определителей. Среди ста определителей от 801 до 900 имеется 7, которым соответствует лишь один единственный род, и 32, 52, 8, 1 определителей, для которых число родов рав-

но соответственно 2, 4, 8, 16; поэтому всего имеется 359 родов, так что среднее количество равно 3,59. Сто отрицательных определителей от  $-801$  до  $-900$  дают 360 родов. Следующие примеры все берутся из отрицательных определителей. В шестнадцатой сотне (от  $-1501$  до  $-1600$ ) среднее количество родов выражается числом 3,89; в двадцать пятой сотне оно равно 4,03, в пятьдесят первой равно 4,24; из шестисот определителей от  $-9401$  до  $-10\,000$  получается число 4,59. Из этих примеров видно, что среднее количество родов возрастает значительно медленнее, чем сами определители. Но, спрашивается, *каков тогда закон этого ряда?* При помощи довольно трудного теоретического исследования, излагать которое здесь было бы слишком долго, было найдено, что среднее число родов для определителя  $+D$  или  $-D$  наиболее точно может быть выражено формулой

$$\alpha \log D + \beta,$$

где  $\alpha$ ,  $\beta$  являются постоянными величинами, причем

$$\alpha \approx \frac{4}{\pi^2} \approx 0,4052847346$$

(где  $\pi$  обозначает половину длины окружности с радиусом 1),

$$\beta = 2\alpha g + 3\alpha^2 h - \frac{1}{6} \alpha \log 2 \approx 0,8830460462,$$

где число  $g$  равно сумме ряда

$$1 - \log(1 + 1) + \frac{1}{2} - \log\left(1 + \frac{1}{2}\right) + \frac{1}{3} - \log\left(1 + \frac{1}{3}\right) + \dots \approx \\ \approx 0,5772156649$$

(ср. Э й л е р, «*Inst. Calc. Diff.*,» р. 444), а число  $h$  — сумме ряда

$$\frac{1}{4} \log 2 + \frac{1}{9} \log 3 + \frac{1}{16} \log 4 + \dots,$$

которая приблизительно равна 0,9375482543. Из этой формулы вытекает, что среднее число родов возрастает в арифметической прогрессии, когда определители растут в геометрической прогрессии. В качестве значений этой формулы для  $D = 850,5$ ;  $1550,5$ ;  $2450,5$ ;  $5050,5$ ;  $9700,5$  мы находим соответственно значения 3,617; 3,86; 4,046,

4,339; 4,604, которые только совсем немного отличаются от приведенных выше средних количеств. Чем больше средний определитель и чем из большего числа определителей вычисляется среднее количество, тем меньше оно отличается от значения, даваемого формулой. При помощи этой формулы можно также приближенно найти сумму чисел, выражающих соответствующие следующим один за другим определителям  $\pm D, \pm(D+1), \dots, \pm(D+m)$  количества родов, если вычислить средние количества, соответствующие отдельным определителям и сложить эти числа; при этом крайние определители  $D$  и  $D+m$  могут сколь угодно отличаться один от другого. Эта сумма равна

$$\alpha [\log D + \log (D+1) + \log (D+2) + \dots + \log (D+m)] + \beta (m+1),$$

или с достаточной точностью равна

$$\alpha [(D+m) \log (D+m) - (D-1) \log (D-1)] + (\beta - \alpha) (m+1).$$

Таким способом для определителей от  $-1$  до  $-100$  сумма количеств родов получается 234,4, в то время как в действительности она равна 233; аналогично, для определителей от  $-1$  до  $-2000$  формула дает значение 7116,6, в то время как в действительности должно быть 7112; для определителей от  $-1$  до  $-3000$  таблица дает число 11166, а формула — число 11167,9; от  $-9001$  до  $-10\,000$ , когда эта сумма равна 4595, формула дает значение 4594,9 — совпадение, которого почти нельзя было ожидать.

## О среднем количестве классов

### 302

Относительно *числа классов* (собственно примитивных положительных, что все время подразумевается) положительные определители ведут себя совершенно не так, как отрицательные; поэтому мы будем рассматривать те и другие отдельно. И те и другие обладают одним и тем же свойством: для заданного определителя в отдельных родах содержится одинаковое число классов, и потому число всех



классов равно произведению числа родов на число классов, содержащихся в отдельном роде.

Что касается, сначала, отрицательных определителей, то число классов, соответствующих многим следующим один за другим определителям  $-D$ ,  $-(D+1)$ ,  $-(D+2)$ , ... образует столь же запутанный ряд, что и число родов. Среднее же число классов (пояснять это понятие нет нужды) растет очень закономерно, что видно из следующих примеров. Сто определителей от  $-501$  до  $-600$  дают 1729 классов, так что среднее количество равно 17,29. Точно так же в пятнадцатой сотне в качестве среднего числа классов получается число 28,26; из 24-й и 25-й сотен получается число 36,28, из 61-й, 62-й и 63-й сотен — число 58,50, из 91-й — 95-й сотен — число 71,56, наконец, из 96-й — 100-й сотен — число 73,54. Эти примеры показывают, что среднее число классов растет хотя и медленнее, чем определители, но все же намного быстрее, чем среднее число родов; при некоторой внимательности мы замечаем, что первое число растет приблизительно так же, как квадратный корень из определителей. И, действительно, теоретическим исследованием мы нашли, что среднее число классов по отношению к определителю  $-D$  очень точно выражается формулой

$$\gamma \sqrt{D} - \delta,$$

где

$$\gamma = \frac{2\pi}{7e} \approx 0,7467183115,$$

$e$  равно сумме ряда

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} + \dots,$$

и

$$\delta = \frac{2}{\pi^2} \approx 0,2026423673,$$

Средние значения, вычисляемые по этой формуле, лишь очень немного отклоняются от тех, которые выше мы привели из таблицы разбиений на классы. При помощи этой формулы можно также приближенно определить сумму средних количеств всех (собственно примитивных положительных) классов, которые соответствуют следующим один за другим определителям  $-D$ ,  $-(D+1)$ ,  $-(D+2)$ , ...

..., —  $(D + m - 1)$ , сколь бы ни отличались один от другого крайние определители, для чего нужно сложить соответствующие этим определителям, согласно формуле, средние количества. Мы получаем, что эта сумма равна

$$\gamma [V\overline{D} + V\overline{D+1} + \dots + V\overline{D+m-1}] - \delta m,$$

или приблизительно равна

$$\frac{2}{3} \gamma \left[ V\overline{\left(D+m-\frac{1}{2}\right)^3} - V\overline{\left(D-\frac{1}{2}\right)^3} \right] - \delta m.$$

Так, например, для ста определителей от  $-1$  до  $-100$  эта сумма по формуле получается равной 481,1, в то время как в действительности она равна 477; тысяча определителей от  $-1$  до  $-1000$  дает, согласно таблице, 15 533 класса, формула же дает 15 551,4; вторая тысяча содержит, согласно таблице, 28 595 классов, формула же дает значение 28 585,7; точно так же, третья тысяча в действительности содержит 37 092 класса, в то время как формула дает 37 074,3; десятая тысяча, согласно таблице, имеет 72 549 классов, в то время как формула дает значение 72 572.

### 303

Таблица отрицательных определителей, на основании которой устанавливается различие соответствующих им разбиений на классы, дает повод и еще ко многим другим специальным замечаниям. Для определителей вида  $-(8n + 3)$  число классов (как тех, которые содержатся во всех родах, так и тех, которые содержатся в отдельных собственно примитивных родах) всегда делится на 3, за исключением лишь определителя  $-3$ , причина чего ясна из п. 256, VI. Для тех определителей, формы которых составляют только один единственный род, число классов всегда нечетно; действительно, так как для такого определителя имеется только один двусторонний класс, именно, главный класс, то число всех остальных классов, которые всегда попарно противоположны, обязательно четно, а потому число всех классов нечетно; впрочем, это последнее свойство имеет место и для положительных определителей. Далее, ряды определителей, которым соответствует

заданное разбиение на классы (т. е. заданное количество как родов, так и классов), всегда оказываются обрывающимися; это неожиданное замечание мы поясним несколькими примерами. (Первая, римская, цифра показывает число собственно примитивных положительных родов, вторая цифра — число классов, содержащихся в каждом отдельном роде; затем следует ряд определителей, которым соответствует такая классификация и отрицательные знаки у которых мы ради краткости отбрасываем.)

|         |                                                                                                        |
|---------|--------------------------------------------------------------------------------------------------------|
| I. 1    | 1, 2, 3, 4, 7                                                                                          |
| II. 3   | 11, 19, 23, 27, 31, 43, 67, 163                                                                        |
| I. 5    | 47, 79, 103, 127                                                                                       |
| I. 7    | 71, 151, 223, 343, 463, 487                                                                            |
| II. 1   | 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58                                                 |
| II. 2   | 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193                     |
| IV. 1   | 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253 |
| VIII. 1 | 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760                    |
| XVI. 1  | 840, 1320, 1365, 1848.                                                                                 |

Аналогично, имеется 20 определителей (наибольший из которых равен — 1423), которым соответствует классификация I.9; 4 определителя (наибольший равен — 1303), которым соответствует классификация I.11, и т. д. Классификациям II.3, II.4, II.5, IV.2 отвечают не больше, чем соответственно 48, 31, 44, 69 определителей, наибольшие из которых равны — 652, —862, —1318, —1012. Так как таблица, из которой взяты эти примеры, продолжается далеко за встречающиеся здесь определители, то представляется бесспорным, что указанные ряды действительно обрываются, и по аналогии мы имеем право распространить это заключение и на любые другие классификации. Так как, например, во всей десятой тысяче определителей нет ни одного, которому соответствовало бы число классов, меньшее чем 24, то в высшей степени вероятно, что классификации I.23;

I.21;..., II.11; II.10;...; IV.5; IV.4; IV.3; VIII.2. уже закончились до —9000, или по крайней мере, что они имеют по другую сторону числа —10 000 очень мало определителей. Однако, *строгие* доказательства этих замечаний оказываются очень трудными. Не менее замечательно то, что все определители, формы которых распадаются на 32 или более родов, имеют в отдельных родах по меньшей мере по два класса, и потому классификации XXXII.1, LXIV.1 и т. д. совершенно не встречаются (наименьшему из этих определителей, равному —9240, соответствует классификация XXXII.2) и представляется весьма вероятным, что с ростом числа родов пропадает все больше и больше классификаций. В этой связи указанные выше 65 определителей, которым соответствуют классификации I.1, II.1, IV.1, VIII.1, XVI.1, оказываются весьма замечательными, и легко видеть, что все они и только они обладают двумя исключительными свойствами, а именно, все принадлежащие им классы форм являются двусторонними, и любые две формы, содержащиеся в одном и том же роде, обязательно эквивалентны как собственно, так и несобственно. Между прочим, эти же 65 чисел (с несколько иной точки зрения, о которой ниже будет упомянуто и которая связана с одним легко доказываемым критерием) были указаны уже Эйлером, «*Nouv. Mém. de l'Ac. de Berlin*», 1776, p. 338.

## 304

Число собственно примитивных классов, которые образуют двойничные формы с *положительным квадратным определителем*  $k^2$ , может быть вообще определено а priori, и равно количеству чисел, которые взаимно просты с числом  $2k$  и меньше чем  $2k$ ; отсюда при помощи несложных рассуждений, которые мы должны здесь опустить, легко найти, что среднее число принадлежащих таким определителям классов для определителя  $k^2$  очень точно выражается числом  $8k/\pi^2$ .

Однако положительные неквадратные определители ведут себя в этом отношении совершенно своеобразно. Именно, в то время как классификации с маленьким числом классов, например, I.1, или I.3, или II.1 и т. д., в случае отрицательных или квадратных определите-

лей встречаются только для небольших, не уходящих далеко значений этих определителей, среди положительных неквадратных определителей, по крайней мере пока они не очень велики, напротив, большая часть обладает такими классификациями, когда в каждом роде имеется только один класс, так что классификации I.3; I.5; II.2; II.3; IV.2 и т. д. весьма редки. Так, например, среди 90 неквадратных определителей, не превосходящих числа 100, имеется 11, 48, 27 определителей, которые имеют соответственно классификацию I.1; II.1; IV.1; только для одного единственного (37) имеет место классификация I.3, два (34 и 82) имеют классификацию II.2 и только один (79) — классификацию II.3. Если, однако, определители возрастают, то большие количества классов встречаются заметно чаще; так, например, среди 96 неквадратных определителей от 101 до 200 два (101 и 197) обладают классификацией I.3; четыре (именно, 145, 146, 178, 194) — классификацией II.2; три (141, 148, 189) — классификацией II.3. Из 197 неквадратных определителей от 801 до 1000 три имеют классификацию I.3, четыре — классификацию II.2, четырнадцать — классификацию II.3, два — классификацию II.5, два — классификацию II.6, пятнадцать — классификацию IV.2, шесть — классификацию IV.3, два — классификацию IV.4, четыре — классификацию VIII.2; остальные 145 определителей имеют только один класс в каждом роде.

Было бы красивой и достойной внимания математиков задачей — определить, по какому закону все реже и реже встречаются определители, обладающие в каждом роде только одним классом; до сих пор мы не можем ни теоретически определить, ни индуктивно с достаточной уверенностью предположить, обрываются ли совершенно в конце концов такие определители (что, однако, представляется мало вероятным), или они становятся по крайней мере бесконечно редкими, или же их частота все ближе подходит к постоянному пределу. Среднее число классов растет лишь немного быстрее, чем среднее число родов, и намного медленнее, чем квадратные корни из определителей; между 800 и 1000 среднее число классов оказывается равным 5,01. Можно было бы добавить к этим замечаниям еще и другое, которое в некотором смысле восстанавливает аналогию между положительными и отрицательными определителями. Именно, мы наш-

ли, что по многим причинам, о которых здесь не будет говоритья подробнее, для положительного определителя  $D$  не столько само число классов, сколько его произведение на логарифм величины  $t + u\sqrt{D}$  (где  $t, u$  обозначают наименьшие, не считая 1 и 0, числа, удовлетворяющие уравнению  $t^2 - Du^2 = 1$ ) аналогично числу классов для отрицательного определителя, и что среднее значение указанного произведения также выражается формулой вида  $m\sqrt{D} - n$ ; однако мы еще не смогли теоретически определить значения постоянных величин  $m, n$ . Если мы имеем право сделать некоторые выводы на основании сравнения нескольких сотен определителей, то оказывается, что значение числа  $m$  не очень отличается от  $2^{1/3}$ . Впрочем, мы оставляем за собой право в другом удобном случае подробнее остановиться на принципах предыдущих исследований относительно средних значений величин, которые возрастают не по аналитическому закону, а лишь непрерывно асимптотически приближаются к такому закону. Теперь мы переходим к другому исследованию, в котором сравниваются между собой различные собственно примитивные классы с одним и тем же определителем, чем мы и завершим этот длинный раздел.

**Особый алгоритм для собственно примитивных классов;  
регулярные и иррегулярные определители и т. д.**

305

**Теорема.** Если  $K$  обозначает главный класс форм с заданным определителем  $D$ , через  $C$  обозначен другой класс из главного рода форм с тем же определителем, и наконец,  $2C, 3C, 4C, \dots$  обозначают классы, которые получаются удвоением, утроением, учетверением и т. д. класса  $C$  (как в п. 249), то в ряду  $C, 2C, 3C, \dots$ , если продолжить его достаточно далеко, в конце концов получится класс, совпадающий с  $K$ , и если предположить, что  $mC$  является первым классом, совпадающим с  $K$ , и что число всех содержащихся в главном роде классов равно  $n$ , то либо  $m = n$ , либо  $m$  является делителем числа  $n$ .

**Доказательство.** I. Так как все классы  $K, C, 2C, 3C, \dots$  обязательно принадлежат главному роду (п. 247), то первые  $n + 1$

классов  $K, C, 2C, \dots, nC$  этого ряда, очевидно, не могут быть все различны. Поэтому либо  $K$  совпадает с каким-нибудь из классов  $C, 2C, 3C, \dots, nC$ , либо по крайней мере два из этих классов будут совпадать между собой. Пусть  $rC = sC$  и  $r > s$ ; тогда также

$$(r-1)C = (s-1)C, (r-2)C = (s-2)C, \dots, (r+1-s)C = C,$$

и потому  $(r-s)C = K$ .

II. Отсюда легко видеть также, что  $m$  или  $= n$ , или  $< n$ , и остается поэтому только показать, что в последнем случае  $m$  является делителем числа  $n$ . Так как классы

$$K, C, 2C, \dots, (m-1)C,$$

совокупность которых мы обозначим через  $\mathfrak{C}$ , в этом случае еще не исчерпывают весь главный род, то пусть  $C'$  — какой-нибудь класс этого рода, не содержащийся в  $\mathfrak{C}$ , обозначим через  $\mathfrak{C}'$  совокупность классов, которые получаются при композиции класса  $C'$  с отдельными классами из  $\mathfrak{C}$ , именно, совокупность

$$C', C' + C, C' + 2C, \dots, C' + (m-1)C.$$

Теперь легко видеть, что все классы в  $\mathfrak{C}'$  отличны как один от другого, так и от всех классов из  $\mathfrak{C}$ , и все они принадлежат главному роду. Если поэтому  $\mathfrak{C}$  и  $\mathfrak{C}'$  полностью исчерпывают этот род, то мы имеем  $n = 2m$ , если же не исчерпывают, то  $2m < n$ . В последнем случае пусть  $C''$  — какой-нибудь не содержащийся ни в  $\mathfrak{C}$ , ни в  $\mathfrak{C}'$  класс главного рода; обозначим через  $\mathfrak{C}''$  совокупность классов, которые получаются при композиции класса  $C''$  с отдельными классами из  $\mathfrak{C}$ , т. е. совокупность

$$C'', C'' + C, C'' + 2C, \dots, C'' + (m-1)C.$$

Тогда легко получается, что все эти классы отличны один от другого и от всех классов из  $\mathfrak{C}$  и  $\mathfrak{C}'$ , и что все они принадлежат главному роду. Если поэтому  $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$  исчерпывают этот род, то  $n = 3m$ , а если нет, то  $n > 3m$ , и в этом случае новый класс, содержащийся в главном роде, но не содержащийся в совокупностях  $\mathfrak{C}, \mathfrak{C}'$  или  $\mathfrak{C}''$ , если рассмотреть его подобным же образом, приводит к выводу, что либо  $n = 4m$ , либо  $n > 4m$  и т. д. А так как  $n$

и  $m$  являются конечными числами, то главный род обязательно рано или поздно будет исчерпан, и  $n$  будет кратностью числа  $m$ , т. е.  $m$  — делителем числа  $n$ .

**Пример.** Если  $D = -356$ ,  $C = (5, 2, 72)^*$ , то мы находим  $2C = (20, 8, 21)$ ,  $3C = (4, 0, 89)$ ,  $4C = (20, -8, 21)$ ,  $5C = (5, -2, 72)$ ,  $6C = (1, 0, 356)$ . Таким образом, здесь  $m = 6$ , а число  $n$  для этого определителя равно 12. Если взять за  $C'$  класс  $(8, 2, 45)$ , то остальными пятью классами из  $\mathfrak{C}'$  будут  $(9, -2, 40)$ ,  $(9, 2, 40)$ ,  $(8, -2, 45)$ ,  $(17, 1, 21)$ ,  $(17, -1, 21)$ .

## 306

Видно, что доказательство предыдущей теоремы совершенно аналогично доказательствам в пп. 45, 49, и действительно, теория умножения классов во всех отношениях имеет тесную связь с предметом, рассматривавшимися в третьем разделе. Однако границы настоящего труда не позволяют изложить здесь указанную теорию с надлежащей полнотой; мы добавим поэтому лишь *несколько замечаний*, опуская также и доказательства, которые потребовали бы более сложного аппарата, и оставим более подробное исследование до другого случая

I. Если ряд  $K, C, 2C, 3C, \dots$  продолжать за  $(m-1)C$ , то снова будут получаться те же самые классы:

$$mC = K, (m+1)C = C, (m+2)C = 2C, \dots,$$

и вообще (если ради краткости рассматривать класс  $K$  как  $0C$ ) классы  $gC, g'C$  будут одинаковы или различны в зависимости от того, сравнимы или нет по модулю  $m$  числа  $g$  и  $g'$ . Класс  $nC$  поэтому всегда совпадает с главным классом  $K$ .

II. Совокупность классов  $K, C, 2C, \dots, (m-1)C$ , которая выше обозначалась через  $\mathfrak{C}$ , мы будем называть **периодом** класса  $C$ , причем это выражение не следует смешивать с рассматривавшимися в пп. 186 и сл. периодами приведенных форм с положительным

---

\* Классы здесь все время представляются содержащимися в них (простейшими) формами.



неквадратным определителем. Очевидно, что при композиции любого числа классов из одного и того же периода снова получается класс, содержащийся в этом же периоде:

$$gC + g'C + g''C + \dots = (g + g' + g'' + \dots)C.$$

III. Так как  $C + (m - 1)C = K$ , то классы  $C$  и  $(m - 1)C$ , и точно так же классы  $2C$  и  $(m - 2)C$ ;  $3C$  и  $(m - 3)C$  и т. д. будут противоположны один другому. Если поэтому  $m$  четно, то класс  $\frac{1}{2}mC$  будет противоположен сам себе и потому будет двусторонним; наоборот, если в  $\mathfrak{E}$ , кроме  $K$ , имеется еще и другой двусторонний класс, например,  $gC$ , то  $gC = (m - g)C$ , и потому  $g = m - g = \frac{1}{2}m$ . Отсюда следует, что если  $m$  четно, то в  $\mathfrak{E}$  не может содержаться других двусторонних классов, кроме  $K$  и  $\frac{1}{2}mC$ , а если  $m$  нечетно, то — кроме единственного класса  $K$ .

IV. Если предположить, что период некоторого содержащегося в  $\mathfrak{E}$  класса  $hC$  состоит из классов

$$K, hC, 2hC, 3hC, \dots, (m' - 1)hC,$$

то  $m'h$  будет, очевидно, наименьшим кратным числа  $h$ , делящимся на  $m$ . Если поэтому  $m$  и  $h$  взаимно просты, то  $m' = m$ , и оба периода будут содержать одни и те же классы, только расположенные различным образом; вообще же, если  $\mu$  обозначает наибольший общий делитель чисел  $m$  и  $h$ , то  $m' = \frac{m}{\mu}$ . Отсюда вытекает, что число классов, содержащихся в периоде некоторого класса из  $\mathfrak{E}$ , или равно  $m$ , или равно некоторому делителю числа  $m$ , причем в  $\mathfrak{E}$  имеют период из  $m$  членов столько классов, сколько чисел среди  $0, 1, 2, \dots, m - 1$  взаимно просто с  $m$ , т. е.  $\varphi(m)$  классов, если использовать обозначение п. 39; вообще же в  $\mathfrak{E}$  имеют период из  $m/\mu$  членов столько классов, сколько чисел среди  $0, 1, 2, \dots, m - 1$  имеют с  $m$  наибольший общий делитель  $\mu$ , т. е., как легко видеть,  $\varphi(m/\mu)$  классов. Поэтому если  $m = n$ , т. е. в  $\mathfrak{E}$  содержит я весь главный род, то в этом роде имеется всего  $\varphi(n)$  классов, периоды которых также содержат весь род, и  $\varphi(e)$  классов, периоды

которых состоят из  $e$  членов, где  $e$  обозначает некоторый делитель числа  $n$ . Этот вывод справедлив всегда, когда в главном роде имеется некоторый класс, период которого состоит из  $n$  членов.

V. При этом же предположении система классов главного рода не может быть расположена более целесообразно, чем если взять какой-нибудь класс, обладающий периодом из  $n$  членов, в некотором смысле за основание, и расположить классы главного рода в том порядке, в котором они следуют в периоде этого класса. Если тогда снабдить главный класс индексом 0, класс, который взят за основание, — индексом 1, и т. д., то простым сложением индексов можно найти, какой класс получается при композиции каких-либо классов главного рода. Здесь приводится пример для определителя — 356, где за основание мы взяли класс (9, 2, 40).

|   |              |   |               |    |               |
|---|--------------|---|---------------|----|---------------|
| 0 | (1, 0, 356)  | 4 | (20, 8, 21)   | 8  | (20, — 8, 21) |
| 1 | (9, 2, 40)   | 5 | (17, 1, 21)   | 9  | (8, 2, 45)    |
| 2 | (5, 2, 72)   | 6 | (4, 0, 89)    | 10 | (5, — 2, 72)  |
| 3 | (8, — 2, 45) | 7 | (17, — 1, 21) | 11 | (9, — 2, 40)  |

VI. Хотя как аналогия с разделом III, так и исследование более чем 200 отрицательных определителей и еще намного большего числа неквадратных положительных определителей делают правдоподобным, что указанное предположение выполняется для *всех* определителей, тем не менее этот вывод был бы неверным и опровергался бы при дальнейшем продолжении таблицы разбиения на классы. Ради краткости мы будем называть *те определители, для которых весь главный род может содержаться в одном единственном периоде, регулярными, а остальные, для которых это невозможно, иррегулярными определителями*. Этот предмет, который оказывается принадлежащим к наиболее скрытым секретам высшей арифметики и дающим простор для труднейших исследований, мы можем здесь проиллюстрировать лишь немногими замечаниями, которым мы предпошлем следующее общее замечание.

VII. Если в главном роде содержатся классы  $C$ ,  $C'$ , периоды которых состоят из  $t$ ,  $t'$  членов, и если  $M$  является наименьшим числом, делящимся на  $t$  и  $t'$ , то в этом роде имеются и классы, периоды

которых содержат  $M$  членов. Если  $M$  разложить на два взаимно простых сомножителя  $r$  и  $r'$ , один из которых ( $r$ ) входит делителем в  $m$ , а другой ( $r'$ ) — в  $m'$  (п. 73), то класс  $\frac{m}{r} C + \frac{m'}{r'} C' = C''$  будет обладать требуемым свойством. Действительно, если мы предположим, что период класса  $C''$  состоит из  $g$  членов, то

$$K = gr C'' = gm C + \frac{grm'}{r'} C' = K + \frac{grm'}{r'} C' = \frac{grm'}{r'} C';$$

поэтому  $grm'/r'$  должно делиться на  $m'$ , т. е.  $gr$  — на  $r'$ , и потому  $g$  — на  $r'$ . Совершенно аналогичным образом мы находим, что  $g$  делится на  $r$ , так что  $g$  делится и на  $rr' = M$ . Но так как, очевидно,  $MC'' = K$ , то и  $M$  будет делиться на  $g$ , и потому обязательно  $M = g$ . Отсюда легко видеть, что *наибольшее* число классов (для заданного определителя), содержащихся в одном периоде, делится на число классов в любом другом периоде (класса из этого же главного рода). Одновременно отсюда же можно вывести метод для отыскания такого класса, период которого наибольший (и потому в случае регулярного определителя охватывает весь главный род), — метод, который совершенно аналогичен методу из пп. 73, 74, хотя на практике вычисления и могут быть связаны со многими искусственными приемами. *Частное от деления числа  $n$  на число классов в наибольшем периоде*, которое для регулярных определителей равно 1, для иррегулярных определителей всегда будет целым числом, большим чем 1, и будет очень удобным средством для характеристики различных степеней иррегулярности; поэтому это частное будет *называться показателем иррегулярности*.

VIII. До сих пор мы не имеем никакого общего правила для того, чтобы сразу отличать регулярные определители от иррегулярных, тем более, что среди последних имеются как простые, так и составные числа; поэтому мы удовлетворимся здесь лишь несколькими специальными замечаниями. Если в главном роде содержится более двух двусторонних классов, то определитель заведомо иррегулярен, и показатель иррегулярности будет четным; если же в каждом роде имеется только один или два двусторонних класса, то определитель или регулярен, или по крайней мере показатель иррегулярности нечетен. Все отрицательные определители вида —  $(216k + 27)$ , за иск-

лючением только одного определителя — 27, иррегулярны, и показатели иррегулярности делятся на 3; это же имеет место для отрицательных определителей вида —  $(1000k + 75)$  и —  $(1000k + 675)$  за исключением лишь определителя — 75, и для бесчисленного множества других. Если показатель иррегулярности равен простому числу  $p$  или по крайней мере делится на  $p$ , то  $n$  делится на  $p^2$ , откуда следует, что если  $n$  не имеет квадратных делителей, то определитель заведомо регулярен. Лишь для положительных *квадратных* определителей  $e^2$  всегда можно сразу узнать, регулярен он или иррегулярен; именно, первое имеет место, когда  $e$  равно либо 1, либо 2, либо нечетному простому числу, либо степени нечетного простого числа; второе — во всех остальных случаях. Среди отрицательных определителей иррегулярные встречаются все чаще по мере возрастания определителей; так, например, во всей первой тысяче определителей иррегулярных имеется тринадцать, а именно (отбрасывая отрицательные знаки), 576, 580, 820, 884, 900, показатель иррегулярности которых равен 2, и 243, 307, 339, 459, 675, 755, 891, 974, показатель иррегулярности которых равен 3 \*; во второй тысяче имеется 13 определителей с показателем иррегулярности 2 и 15 определителей с показателем иррегулярности 3; в десятой тысяче имеется 31 определитель с показателем иррегулярности 2 и 32 определителя с показателем иррегулярности 3. Имеются ли до —10 000 определители с показателями иррегулярности, большими чем 3, я еще не могу узнать; по другую же сторону этой границы могут получиться любые заданные показатели. То, что отношение частоты иррегулярных отрицательных определителей к частоте регулярных по мере роста определителей все более и более приближается к постоянному значению, в высшей степени правдоподобно, и определение этого отношения было бы задачей, достойной внимания математиков. Среди положительных неквадратных определителей иррегулярные встречаются намного реже; таких определителей, у которых показатель иррегулярности четный, заведомо имеется бесконечно много (например, определитель 3026, для которого этот показатель равен 2); также представляется несомненным, что имеются и определители, у которых пока-

---

\* Ср. дополнения в конце «Исследований».

затель иррегулярности нечетен, хотя мы должны признать, что нам еще ни один такой определитель не известен.

IX. Относительно наиболее удобного расположения системы классов, которые содержатся в главном роде в случае иррегулярного определителя, мы здесь, ради краткости, говорить не будем; заметим только, что так как одного основания в этом случае недостаточно, то необходимо брать два или даже еще большее число классов, при умножении и композиции которых получаются уже все остальные. При этом получаются двойные и кратные индексы, польза которых состоит примерно в том же, в чем состоит и польза простых индексов при регулярных определителях. Однако подробнее мы рассмотрим этот вопрос при другом подходящем случае.

X. Наконец, заметим, что так как все рассмотренные в этом и предыдущем пунктах свойства в основном зависят от числа  $n$ , которое представляет собой нечто подобное числу  $p - 1$  из раздела III, то это число  $n$  заслуживает самого пристального внимания, и потому было бы весьма желательно открыть общую связь между ним и определителем, которому оно принадлежит. В этом очень важном вопросе мы тем более не должны отчаиваться, что по крайней мере для отрицательных определителей уже известно представление в виде аналитической формулы для среднего значения произведения числа  $n$  на число родов, которое может быть определено непосредственно (п. 302) \*.

### 307

Исследования предыдущего пункта охватывают только классы главного рода; этих исследований, таким образом, достаточно для положительных определителей, у которых вообще имеется только один род, и, если не рассматривать отрицательных родов, для отрицательных определителей, имеющих только один положительный род. Поэтому нам остается только добавить кое-что еще относительно остальных (собственно примитивных) родов.

I. Если в роде  $G'$ , который отличен от главного рода  $G$  (с тем же определителем), имеется хотя бы один двусторонний класс, то их в

---

\* Ср. дополнения в конце «Исследований».

этом роде столько же, сколько и в  $G$ . Пусть в роде  $G$  содержатся двусторонние классы  $L, M, N, \dots$  (среди которых находится также и главный класс  $K$ ), а в роде  $G'$  — двусторонние классы  $L', M', N', \dots$ , и пусть совокупность первых обозначена через  $A$ , а совокупность последних — через  $A'$ . Так как все классы  $L + L', M + L', N + L', \dots$ , очевидно, двусторонние, различны между собой и принадлежат роду  $G'$ , т. е. должны содержаться в совокупности  $A'$ , то число классов в  $A'$  заведомо не может быть меньше чем в  $A$ ; а так как, точно так же, классы  $L' + L', M' + L', N' + L' — двусторонние, различны между собой и принадлежат роду  $G$ , т. е. содержатся в  $A$ , то число классов в  $A$  не может быть меньше чем в  $A'$ . Поэтому количества классов в  $A$  и  $A'$  обязательно равны между собой.$

II. Так как число всех двусторонних классов равно числу родов (пп. 261, 287, III), то если в  $G$  имеется только один двусторонний класс, то и в каждом роде может содержаться только один двусторонний класс; если же в  $G$  существует два двусторонних класса, то в половине всех родов их имеется по два, а в другой половине их вообще нет; и если в  $G$  содержится несколько, скажем,  $a$  двусторонних классов \*, то  $a$ -я часть родов содержит по  $a$  двусторонних классов каждый, а остальные роды вообще не содержат таких классов.

III. Пусть в случае, когда  $G$  содержит два двусторонних класса, через  $G, G', G'', \dots$  обозначены те роды, которые имеют по два двусторонних класса, а через  $H, H', H'', \dots$  — те роды, которые не содержат двусторонних классов; обозначим совокупность первых через  $\mathfrak{G}$ , а совокупность последних через  $\mathfrak{H}$ . Так как при композиции двух двусторонних классов всегда получается снова двусторонний класс (п. 249), то, очевидно, что при композиции двух родов из  $\mathfrak{G}$  всегда снова получается род из  $\mathfrak{G}$ . Отсюда следует, далее, что при композиции рода из  $\mathfrak{G}$  с родом из  $\mathfrak{H}$  получается род из  $\mathfrak{H}$ . Действительно. если, например, род  $G' + H$  принадлежал бы не к  $\mathfrak{H}$ , а к  $\mathfrak{G}$ , то к  $\mathfrak{G}$  должен был бы принадлежать и род  $G' + H + G'$ , что невозможно, так как  $G' + G' = G$  и потому  $G' + H + G' = H$ .

---

\* Это может иметь место только для иррегулярных определителей, причем  $a$  обязательно должно быть степенью числа 2.

Наконец, мы легко заключаем, что роды  $G + H$ ,  $G' + H$ ,  $G'' + H$ , ... вместе с родами  $H + H$ ,  $H' + H$ ,  $H'' + H$ , ... все различны между собой, и потому охватывают всю совокупность родов из  $\mathfrak{G}$  и  $\mathfrak{H}$ ; но не только что доказанному все роды  $G + H$ ,  $G' + H$ ,  $G'' + H$ , ... принадлежат к  $\mathfrak{H}$ , и потому исчерпывают эту совокупность, а, значит, все остальные роды  $H + H$ ,  $H' + H$ ,  $H'' + H$ , ... принадлежат к  $\mathfrak{G}$ , т. е. при композиции двух родов из  $\mathfrak{H}$  всегда получается род из  $\mathfrak{G}$ .

IV. Если  $E$  есть класс из рода  $V$ , отличного от главного рода  $G$ , то все классы  $2E$ ,  $4E$ ,  $6E$ , ..., очевидно, будут принадлежать к  $G$ , а классы  $3E$ ,  $5E$ ,  $7E$ , ... — к  $V$ . Поэтому, если период класса  $2E$  состоит из  $m$  членов, то в ряде  $E$ ,  $2E$ ,  $3E$ , ... с классом  $K$  будет, очевидно, совпадать класс  $2mE$  и никакой более ранний, т. е. период класса  $E$  будет состоять из  $2m$  членов. Поэтому число членов в периоде каждого класса, не принадлежащего главному роду, либо равно  $2n$ , либо является делителем числа  $2n$ , где  $n$  обозначает число классов в отдельном роде.

V. Пусть  $C$  — заданный класс главного рода  $G$ ,  $E$  — класс рода  $V$ , при удвоении которого получается  $C$  (такой всегда существует, согласно п. 286), и пусть, далее,  $K$ ,  $K'$ ,  $K''$ , ..., — все двусторонние собственно примитивные классы (с тем же определителем). Тогда всевозможными классами, при удвоении которых получается  $C$ , являются классы  $E (= E + K)$ ,  $E + K'$ ,  $E + K''$ , ..., совокупность которых мы обозначим через  $\Omega$ ; число этих классов равно числу двусторонних классов, т. е. равно числу родов. Ясно, что среди классов из  $\Omega$  роду  $V$  принадлежит столько, сколько имеется двусторонних классов в  $G$ ; поэтому, если обозначить их число через  $a$ , то в каждом роде будет, очевидно, содержаться или  $a$  классов из  $\Omega$ , или ни одного. Из этого легко видеть, что если  $a = 1$ , то в каждом роде содержится один класс из  $\Omega$ ; далее, что если  $a = 2$ , то половина всех родов содержит по два класса из  $\Omega$ , а другая половина не содержит таких классов, причем либо первая половина совпадает целиком с  $\mathfrak{G}$ , а вторая половина — целиком с  $\mathfrak{H}$  либо вторая совпадает с  $\mathfrak{G}$ , а первая — с  $\mathfrak{H}$  ( $\mathfrak{G}$  и  $\mathfrak{H}$  имеют то же значение, что и выше, в III). Если  $a$  еще больше, то классы из  $\Omega$  будут содержать  $a$ -я часть всех родов (причем каждый из них — по  $a$  классов).



VI. Если мы теперь предположим, что  $C$  является классом, период которого состоит из  $n$  членов, то легко видеть, что в случае, когда  $a = 2$  и потому  $n$  четно, ни один класс из  $\Omega$  не может принадлежать к  $G$  (действительно, в противном случае такой класс содержался бы в периоде класса  $C$ ; если поэтому обозначить его через  $rC$ , так что  $2rC = C$ , то имело бы место  $2r \equiv 1 \pmod{n}$ , что невозможно); а так как  $G$  принадлежит к  $\mathfrak{G}$ , то все классы из  $\Omega$  обязательно должны распределяться среди родов из  $\mathfrak{H}$ . Отсюда следует, так как всего в  $G$  (для регулярного определителя) имеется  $\varphi(n)$  классов, имеющих периоды из  $n$  членов, что в случае, когда  $a = 2$ , в каждом роде из  $\mathfrak{H}$  находится  $2\varphi(n)$  классов, периоды которых имеют  $2n$  членов и потому охватывают как их собственный род, так и главный род; если же  $a = 1$ , то в каждом роде, отличном от главного, имеется  $\varphi(n)$  таких классов.

VII. На этих замечаниях мы основываем следующий *метод наиболее целесообразного определения системы всех собственно примитивных классов для каждого данного регулярного (ибо иррегулярные мы полностью оставляем в стороне) определителя*. Выберем по желанию произвольный класс  $E$ , период которого состоит из  $2n$  членов и потому содержит как его собственный род, который мы обозначим через  $V$ , так и главный род; классы обоих этих родов мы расположим так, как они следуют в этом периоде. Таким образом, цель уже будет достигнута, если других родов, кроме этих двух, нет, или оказывается ненужным их определять (например, в случае такого отрицательного определителя, для которого имеется только два положительных рода). Если же нужно определить четыре или больше родов, то остальные получаются следующим образом. Если  $V'$  — какой-нибудь род из других, и  $V + V' = V''$ , то в  $V'$  и  $V''$  имеются два двусторонних класса (либо в каждом из них по одному, либо в одном два, а в другом ни одного); если выбрать любой класс  $A$  из этих двух, то легко видеть, что если комбинировать  $A$  с отдельными классами из  $G$  и  $V$ , то мы получим  $2n$  различных принадлежащих к  $V'$  и  $V''$  и потому полностью исчерпывающих эти роды классов; тем самым описываются и эти роды. Если, кроме этих четырех родов, имеются еще и другие, то пусть  $V'''$  — один из них, и пусть, далее,  $V''', V''''$ ,  $V'''''$  — те



роды, которые получаются при композиции рода  $V'''$  с  $V$ ,  $V'$  и  $V''$ . Эти четыре рода  $V'''$ ,  $V'''$ ,  $V'''$ ,  $V'''$  содержат четыре двусторонних класса, и ясно, что если один из них,  $A'$ , выбрать и скомбинировать с отдельными классами из  $G$ ,  $V$ ,  $V'$ ,  $V''$ , то получатся все классы из  $V'''$ , ...,  $V'''$ . Если имеется еще больше классов, то мы продолжаем таким же образом, пока не исчерпаем их все. Очевидно, что если число всех подлежащих определению родов равно  $2^\mu$ , то всего нужно будет иметь  $2^{\mu-1}$  двусторонних классов и каждый класс из этих родов будет получаться либо умножением класса  $E$ , либо композицией некоторого класса, получающегося таким умножением, с одним или несколькими двухсторонними классами. Для пояснения этих правил мы дадим здесь два примера; относительно пользы таких конструкций и искусственных приемов, благодаря которым работа может быть облегчена, мы здесь ничего добавлять не будем.

\* \* \*

### I. Определитель — 161

Четыре положительных рода; в каждом из них по четыре класса

| $G$                                                                                                                | $V$                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| $1, 4; R7; R23$<br>$(1, 0, 161) = K$<br>$(9, 1, 18) = 2E$<br>$(2, 1, 81) = 4E$<br>$(9, -1, 18) = 6E$               | $3, 4; N7, R23$<br>$(3, 1, 54) = E$<br>$(6, -1, 27) = 3E$<br>$(6, 1, 27) = 5E$<br>$(3, -1, 54) = 7E$                   |
| $V'$                                                                                                               | $V''$                                                                                                                  |
| $3, 4; R7; N23$<br>$(7, 0, 23) = A$<br>$(11, -2, 15) = A + 2E$<br>$(14, 7, 15) = A + 4E$<br>$(11, 2, 15) = A + 6E$ | $1, 4; N7; N23$<br>$(10, 3, 17) = A + E$<br>$(5, 2, 33) = A + 3E$<br>$(5, -2, 33) = A + 5E$<br>$(10, -3, 17) = A + 7E$ |

## II. Определитель — 546

Восемь положительных родов; в каждом из них по три класса

| $G$                                                                                                                                                                                                | $V$                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1 и 3, 8; <math>R3</math>; <math>R7</math>; <math>R13</math><br/> <math>(1, 0, 546) = K</math><br/> <math>(22, -2, 25) = 2E</math><br/> <math>(22, 2, 25) = 4E</math></p>                       | <p>3 и 7, 8; <math>N3</math>; <math>N7</math>; <math>N13</math><br/> <math>(5, 2, 110) = E</math><br/> <math>(21, 0, 26) = 3E</math><br/> <math>(5, -2, 110) = 5E</math></p>                              |
| $V'$                                                                                                                                                                                               | $V''$                                                                                                                                                                                                     |
| <p>1 и 3, 8; <math>N3</math>, <math>R7</math>; <math>N13</math><br/> <math>(2, 0, 273) = A</math><br/> <math>(11, -2, 50) = A + 2E</math><br/> <math>(11, 2, 50) = A + 4E</math></p>               | <p>5 и 7, 8; <math>R3</math>; <math>N7</math>, <math>R13</math><br/> <math>(10, 2, 55) = A + E</math><br/> <math>(13, 0, 42) = A + 3E</math><br/> <math>(10, -2, 55) = A + 5E</math></p>                  |
| $V'''$                                                                                                                                                                                             | $V''''$                                                                                                                                                                                                   |
| <p>1 и 3, 8; <math>N3</math>; <math>N7</math>; <math>R13</math><br/> <math>(3, 0, 182) = A'</math><br/> <math>(17, 7, 35) = A' + 2E</math><br/> <math>(17, -7, 35) = A' + 4E</math></p>            | <p>5 и 7, 8; <math>R3</math>; <math>R7</math>; <math>N13</math><br/> <math>(15, -3, 37) = A' + E</math><br/> <math>(7, 0, 78) = A' + 3E</math><br/> <math>(15, 3, 37) = A' + 5E</math></p>                |
| $V'''''$                                                                                                                                                                                           | $V''''''$                                                                                                                                                                                                 |
| <p>1 и 3, 8; <math>R3</math>; <math>N7</math>; <math>N13</math><br/> <math>(6, 0, 91) = A + A'</math><br/> <math>(19, 9, 33) = A + A' + 2E</math><br/> <math>(19, -9, 33) = A + A' + 4E</math></p> | <p>5 и 7, 8; <math>N3</math>; <math>R7</math>; <math>R13</math><br/> <math>(23, 11, 29) = A + A' + E</math><br/> <math>(14, 0, 39) = A + A' + 3E</math><br/> <math>(23, -11, 29) = A + A' + 5E</math></p> |

---

## РАЗДЕЛ VI

### РАЗЛИЧНЫЕ ПРИМЕНЕНИЯ ПРЕДЫДУЩИХ ИССЛЕДОВАНИЙ

308

Во многих местах до этого мы уже касались того, насколько высшая арифметика богата истинами, находящими применение также и в других частях математики; мы считаем, однако, небесполезным специально рассмотреть некоторые приложения, которые заслуживают более подробного изложения, не столько для того, чтобы исчерпать этот предмет, которым легко могли бы быть заполнены многие тома, сколько для того, чтобы на нескольких примерах пролить на него более яркий свет. В настоящем разделе мы сначала будем говорить о разложении дробей на более простые, затем о превращении обыкновенных дробей в десятичные; после этого мы изложим один новый метод исключения, который служит для решения неопределенных уравнений второй степени; наконец, мы укажем простые новые методы для того, чтобы отличать простые числа от составных и получать сомножители последних. В следующем же разделе мы дадим обоснование общей теории одного специального и очень часто используемого в общем анализе класса функций, поскольку она находится в теснейшей связи с высшей арифметикой, и, в частности, попытаемся обогатить новыми фактами теорию деления круга, из которой до сих пор были известны лишь первые элементы.

## Разложение дробей на более простые

309

**Задача.** Дробь  $m/n$ , знаменатель которой есть произведение двух взаимно простых чисел  $a, b$ , разложить на две другие, знаменателями которых являются  $a$  и  $b$ .

**Решение.** Если искомые дроби суть  $x/a, y/b$ , то должно быть  $bx + ay = m$ ; поэтому  $x$  является корнем сравнения  $bx \equiv m \pmod{a}$ , который мы можем найти на основании раздела II;  $y$  же будет равен  $(m - bx)/a$ .

Известно, впрочем, что сравнение  $bx \equiv m \pmod{a}$  обладает бесконечно многими, но сравнимыми по модулю  $a$  корнями, но что имеется только один положительный корень, который меньше, чем  $a$ ; может, однако, случиться, что  $y$  будет отрицательным. Вряд ли нужно указывать на то, что  $y$  может быть также определен при помощи сравнения  $ay \equiv m \pmod{b}$ , а  $x$  — из равенства  $x = \frac{m - ay}{b}$ . Если, например, дана дробь  $^{58}/_{77}$ , то значением выражения  $\frac{58}{11} \pmod{7}$  является число 4, и потому  $^{58}/_{77}$  распадается на  $\frac{4}{7} + \frac{2}{11}$ .

310

Если дана дробь  $m/n$ , знаменатель  $n$  которой является произведением любого количества попарно взаимно простых чисел  $a, b, c, d, \dots$ , то, согласно предыдущему пункту, ее можно сначала разложить на две дроби со знаменателями  $a$  и  $bcd\dots$ ; последнюю снова разложить на две и т. д., до тех пор, пока наконец заданная дробь не будет приведена к виду

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \dots$$

Числители  $\alpha, \beta, \gamma, \delta, \dots$  можно, очевидно, предполагать положительными и меньшими, чем их знаменатели, за исключением последнего, который, после того, как остальные определены, больше уже не является произвольным и может оказаться отрицательным, а также бóльшим знаменателя (поскольку мы не предполагаем, что

$m < n$ ). Тогда по большей части будет целесообразным привести его к виду  $\frac{\varepsilon}{e} \mp k$ , где  $\varepsilon$  — положительное число, меньшее чем  $e$ , а  $k$  — целое число. Наконец, ясно, что числа  $a, b, c, \dots$  можно считать либо простыми, либо степенями простых чисел.

**Пример.** Дробь  $^{391}/_{924}$ , знаменатель которой равен  $4 \cdot 3 \cdot 7 \cdot 11$ , раскладывается, таким образом, на  $\frac{1}{4} + \frac{40}{231}$ ;  $\frac{40}{231}$  на  $\frac{2}{3} - \frac{38}{77}$ ;  $-\frac{38}{77}$  на  $\frac{1}{7} - \frac{7}{11}$ , так что если написать  $\frac{4}{11} - 1$  вместо  $-\frac{7}{11}$ , то получится  $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$ .

### 311

Дробь  $m/n$  может быть *только одним способом* приведена к такому виду  $\frac{\alpha}{a} + \frac{\beta}{b} + \dots \mp k$ , что  $\alpha, \beta, \dots$  положительны и соответственно меньше чем  $a, b, \dots$ ; действительно, если мы предположим, что

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \dots \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \dots \mp k',$$

и что  $\alpha', \beta', \dots$  тоже положительные числа, меньшие соответственно чем  $a, b, \dots$ , то обязательно должно быть  $\alpha = \alpha', \beta = \beta', \gamma = \gamma', \dots, k = k'$ . Именно, если умножить равенство на  $n = abc\dots$ , то, очевидно, будет иметь место  $m \equiv \alpha bcd\dots \equiv \alpha' bcd\dots \pmod{a}$ , и потому, так как  $bcd\dots$  взаимно просто с  $a$ , обязательно  $\alpha \equiv \alpha'$ , и тем самым  $\alpha = \alpha'$ , и точно так же  $\beta = \beta'$  и т. д., откуда само по себе следует и  $k = k'$ . Так как теперь совершенно безразлично, для какого знаменателя сначала находится числитель, то ясно, что все числители могут быть найдены так же, как  $\alpha$  в предыдущем пункте, именно,  $\beta$  — из сравнения  $\beta acd\dots \equiv m \pmod{b}$ ,  $\gamma$  из  $\gamma abd\dots \equiv m \pmod{c}$  и т. д. Сумма всех так найденных дробей либо равна заданной дроби  $m/n$ , либо разность между ними является целым числом  $k$ , так что мы получаем таким путем одновременно и проверку правильности вычислений. Так, в примере предыдущего пункта значения выражений  $\frac{391}{231} \pmod{4}$ ,  $\frac{391}{308} \pmod{3}$ ,  $\frac{391}{132} \pmod{7}$ ,  $\frac{391}{84} \pmod{11}$

тотчас дают соответствующие знаменателям 4, 3, 7, 11 числители 1, 2, 1, 4, и мы находим, что сумма этих дробей превосходит заданную дробь на единицу.

## Превращение обыкновенных дробей в десятичные

312

**Определение.** Если обыкновенная дробь превращается в десятичную, то мы будем называть ряд десятичных чисел\* (за исключением целого числа, если оно имеется), независимо от того, конечен он или уходит в бесконечность, мантисой дроби, употребляя в новом значении выражение, применяемое обычно только в логарифмах. Так, например, мантисса дроби  $\frac{1}{8}$  равна 125, мантисса дроби  $\frac{35}{16}$  равна 1875, мантисса дроби  $\frac{2}{37}$  равна 054054... и т. д. до бесконечности.

Из этого определения тотчас же вытекает, что дроби  $l/n$ ,  $m/n$  с одним и тем же знаменателем имеют одинаковые или различные мантиссы в зависимости от того, сравнимы или нет числители  $l$ ,  $m$  по модулю  $n$ . Конечная мантисса не изменяется, если справа к ней добавлять любое число нулей. Мантиссу дроби  $10m/n$  мы получим, если отбросим первую цифру у мантиссы дроби  $m/n$ , и, вообще, мантиссу дроби  $10^v m/n$  мы найдем, отбросив  $v$  первых цифр у мантиссы дроби  $m/n$ . Мантисса дроби  $1/n$  сразу начинается со значащей (т. е. отличной от нуля) цифры, если  $n$  не больше чем 10; если же  $n > 10$  и не является степенью числа 10, а число цифр, из которых состоит  $n$ , равно  $k$ , то  $k-1$  первых цифр мантиссы будут нулями, и только следующая,  $k$ -я цифра будет значащей. Отсюда легко видеть, что если  $l/n$ ,  $m/n$  имеют различные мантиссы (т. е. если  $l$ ,  $m$  несравнимы по модулю  $n$ ), то эти мантиссы заведомо не могут совпадать в первых  $k$  цифрах, а обязательно отличаются по крайней мере в  $k$ -й цифре.

---

\* Ради краткости мы ограничимся в дальнейшем исследовании обычной десятичной системой, так как она легко может быть преобразована в любую систему.

## 313

**Задача.** Пусть заданы знаменатель дроби  $t/n$  и первые  $k$  цифр ее мантиссы; нужно найти числитель  $t$ , который мы предполагаем меньшим чем  $n$ .

**Решение.** Рассмотрим эти  $k$  цифр как целое число, умножим его на  $n$  и разделим произведение на  $10^k$  (т. е. отделим последние  $k$  цифр). Если частное есть целое число (т. е. если отделенные цифры являются нулями), то это частное и является искомым числителем, и заданная мантисса полна; если же нет, то искомый числитель является следующим целым числом, т. е. увеличенным на единицу частным с отброшенными следующими десятичными знаками. Обоснование этого правила настолько очевидно из наших замечаний в конце предыдущего пункта, что не требует дальнейших пояснений.

**Пример.** Если известно, что двумя первыми цифрами мантиссы дроби со знаменателем 23 являются 69, то мы получаем произведение  $23 \cdot 69 = 1587$ ; если отбросить от него две последние цифры и прибавить 1, мы получим, что искомый числитель равен 16.

## 314

Мы начнем с рассмотрения таких дробей, у которых знаменатели являются простыми числами или степенями простых чисел, и затем покажем, как остальные дроби могут быть сведены к этим. Прежде всего мы тотчас же заметим, что мантисса дроби  $a/p^\mu$  (относительно числителя  $a$  которой мы все время предполагаем, что он не делится на простое число  $p$ ) конечна и состоит из  $\mu$  цифр, если  $p = 2$  или  $p = 5$ ; в первом случае эта мантисса, рассматриваемая как целое число, равна  $5^\mu a$ , а во втором равна  $2^\mu a$ . Это настолько ясно, что не требует пояснений.

Если же  $p$  — другое простое число, то  $10^r a$  никогда не будет делиться на  $p^\mu$ , сколь большое  $r$  мы бы ни брали, откуда немедленно следует, что мантисса дроби  $F = \frac{a}{p^\mu}$  обязательно продолжается до бесконечности. Если мы предположим, что  $10^e$  есть наименьшая степень числа 10, которая сравнима с единицей по модулю

$p^\mu$  (ср. раздел III, где мы показали, что  $e$  либо равно числу  $(p-1)p^{\mu-1}$ , либо является его делителем), то легко убедиться, что также и  $10^e a$  будет первым числом в ряду чисел  $10a, 100a, 1000a, \dots$ , которое сравнимо с  $a$  по этому же модулю. Но так как, согласно п. 312, мантиссы дробей  $10a/p^\mu, 100a/p^\mu, \dots, 10^e a/p^\mu$  получаются, если отбрасывать у мантиссы дроби  $F$  соответственно одну, две,  $\dots, e$  первых цифр, то ясно, что в этой мантиссе после первых  $e$  цифр, и не раньше, снова повторяются прежние цифры. Эти первые  $e$  цифр, из бесконечного повторения которых образована мантисса, мы будем называть периодом этой мантиссы или дроби  $F$ , и очевидно, что величина периода, т. е. число цифр, из которых он состоит, и которое равно  $e$ , совершенно не зависит от числителя  $a$  и определяется только знаменателем. Так, например, период дроби  $1/11$  равен 09, период дроби  $3/7$  равен 428571.

## 315

Поэтому, если мы знаем период некоторой дроби, мы можем продолжить мантиссу до любого количества цифр. Далее получается, что если  $b \equiv 10^\lambda a \pmod{p^\mu}$ , то период дроби  $b/p^\mu$  мы получим, если первые  $\lambda$  цифр дроби  $F$  (где мы предполагаем  $\lambda < e$ , что допустимо) напишем после остальных  $e - \lambda$  цифр, и что тем самым мы одновременно с периодом дроби  $F$  имеем также периоды всех дробей, числители которых сравнимы по модулю  $p^\mu$  с числами  $10a, 100a, 1000a, \dots$ . Например, так как  $6 \equiv 3 \cdot 10^2 \pmod{7}$ , то из периода дроби  $3/7$  тотчас же находится период дроби  $6/7$ , равный 857 142.

Если поэтому для модуля  $p^\mu$  число 10 является первообразным корнем (пп. 57, 89), то в случае, когда за основание взято число 10, из периода дроби  $1/p^\mu$  тотчас же можно получить период всякой другой дроби  $t/p^\mu$  (у которой числитель  $t$  не делится на  $p$ ), отделив у первого из упомянутых периодов слева и приписав затем к нему справа столько цифр, сколько единиц содержит индекс числа  $t$ , если за основание взято число 10. Отсюда явствует, почему в этом случае в таблице 1 всегда берется за основание число 10 (п. 72).

Если же 10 не является первообразным корнем, то из периода дроби  $1/p^\mu$  могут быть получены периоды только тех дробей,



числители которых сравнимы по модулю  $p^\mu$  с некоторыми степенями числа 10. Пусть  $10^e$  — наинизшая степень числа 10, которая сравнима с единицей по модулю  $p^\mu$ , далее,  $(p-1)p^{\mu-1} = ef$ , и за основание взят такой первообразный корень  $r$ , что индекс числа 10 равен  $f$  (п. 71). Таким образом, в этой системе числители дробей, периоды которых могут быть выведены из периода дроби  $1/p^\mu$ , имеют индексы  $f, 2f, 3f, \dots, ef-f$ ; аналогично, из периода дроби  $r/p^\mu$  могут быть найдены периоды дробей, числители которых  $10r, 100r, 1000r, \dots$  соответствуют индексам  $f+1, 2f+1, 3f+1, \dots$ ; из периода дроби с числителем  $r^2$  (индекс которого равен 2) получаются периоды дробей с числителями, индексами которых являются  $f+2, 2f+2, 3f+2, \dots$ , и вообще, из периода дроби с числителем  $r^i$  могут быть выведены периоды дробей с числителями, индексами которых являются  $f+i, 2f+i, 3f+i, \dots$ . Из этого мы легко заключаем, что если только мы имеем периоды дробей с числителями  $1, r, r^2, r^3, \dots, r^{f-1}$ , то все остальные могут быть выведены отсюда простыми перестановками по следующему правилу.

Пусть в системе, в которой за основание взято число  $r$ , индекс числителя  $m$  заданной дроби  $m/p^\mu$  равен  $i$  (это число мы предполагаем меньшим чем  $(p-1)p^{\mu-1}$ ); положим (деля на  $f$ )  $i = \alpha f + \beta$ , где  $\alpha, \beta$  являются целыми положительными числами (или также равны 0) и  $\beta < f$ . Тогда период дроби  $m/p^\mu$  получится из периода дроби с числителем  $r^\beta$  (который, следовательно, равен 1, если  $\beta = 0$ ), если первые  $\alpha$  цифр в нем поставить после остальных (тем самым, период останется неизменным, если  $\alpha = 0$ ). Это достаточно поясняет, почему при построении таблицы 1 мы следовали правилу, изложенному в п. 72.

### 316

По этим принципам мы для всех знаменателей вида  $p^\mu$ , меньших 1000, составили таблицу необходимых периодов, которую мы целиком или даже в еще продолженном виде опубликуем в свое время. Здесь в качестве примера достаточно продолженной лишь до 100 таблицы\* и пояснения к ней почти не нужны. Для тех знаменателей, для которых 10 является первообразным корнем, она дает периоды

\* Таблица 3; помещена на стр. 578—579.—Прим. ред.

дробей с числителем 1 (именно, для 7, 17, 19, 23, 29, 47, 59, 61, 97), для остальных знаменателей — периоды, соответствующие  $f$  числителям  $1, r, r^2, \dots, r^{f-1}$ , которые указываются приписанными числами (0), (1), (2), ...; в качестве основания  $r$  всегда берется тот же первообразный корень, что и в таблице 1. Поэтому период каждой дроби, знаменатель которой содержится в этой таблице, может быть найден по правилу из предыдущего пункта, после того как при помощи таблицы 1 найден индекс числителя. Впрочем, для таких маленьких знаменателей задача столь же легко может быть решена и без таблицы 1, если мы простым делением вычислим столько первых цифр искомой мантиссы, сколько, согласно п. 313, их необходимо иметь, чтобы ее можно было отличить от любой другой мантиссы для этого же знаменателя (для таблицы 3 не более чем две цифры), и тщательно пересмотрим все соответствующие этому знаменателю периоды, пока не найдем наших начальных цифр, которые точно указывают начало периода; нужно, однако, указать на то, что эти цифры могут также оказаться разделенными, так что первая (или несколько первых) будет образовывать конец некоторого периода, а остальные (или оставшаяся) — его начало.

**Пример.** Найдем период дроби  $12/19$ . Здесь для модуля 19 мы имеем (см. таблицу 1)  $\text{ind } 12 = 2 \text{ ind } 2 + 3 \text{ ind } 3 = 39 \equiv 3 \pmod{18}$  (п. 57). Поэтому, так как для этого случая имеется только один период, соответствующий числителю 1, нужно переставить в конец три его первые цифры, откуда и получается искомый период: 631578947368421052. Так же легко можно было бы найти начало периода по двум первым цифрам 63.

Если мы хотим найти период дроби  $45/53$ , то, для модуля 53,  $\text{ind } 45 = 2 \text{ ind } 3 + \text{ind } 5 = 49$ ; количество периодов здесь равно  $4 = f$ , и  $49 = 12f + 1$ ; поэтому в периоде, обозначенном через (1), нужно первые 12 цифр поставить после остальных, и искомый период есть 8490566037735. В этом случае первые цифры 8 и 4 в таблице отделены одна от другой.

*Заметим еще, что при помощи таблицы 3 можно также найти число, которое для заданного модуля (фигурирующего в таблице под названием знаменателя) соответствует заданному индексу, что мы уже в п. 59 обещали показать. Действительно, согласно предыдущему*

можно, очевидно, найти период дроби, числитель которой (если он даже и неизвестен) соответствует заданному индексу; достаточно взять из таблицы столько первых цифр этого периода, сколько цифр имеет знаменатель; из них, в соответствии с п. 313, мы найдем числитель, т. е. искомое число, соответствующее заданному индексу.

## 317

Согласно изложенному, может быть без вычислений найдено любое число цифр мантиссы всякой дроби, знаменатель которой является простым числом или степенью простого числа, не превосходящей границ таблицы; однако на основании исследований в начале этого раздела применение таблицы распространяется еще гораздо дальше и охватывает все дроби, знаменатели которых являются произведениями простых чисел или степеней простых чисел, если эти степени не превосходят ее границ. Действительно, так как такая дробь может быть разложена на дроби, знаменателями которых являются эти сомножители, а эти дроби могут быть превращены в десятичные до любого знака, то остается только объединить последние в сумму. Впрочем, вряд ли нужно даже указывать на то, что последняя цифра этой суммы может оказаться меньше правильной цифры; но очевидно, что разница не может превосходить столько единиц, сколько складывается отдельных дробей, так что все будет хорошо, если их вычислить на несколько знаков дальше того места, до которого должно быть точным выражение для заданной дроби. Для примера мы рассмотрим дробь  $F = \frac{6\ 099\ 380\ 351}{1\ 271\ 808\ 720}^*$ , знаменатель которой есть произведение чисел 16, 9, 5, 49, 13, 47, 59. Согласно изложенным выше принципам мы находим:  $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$ , и эти частичные дроби следующим образом превращаются в десятичные:

$$1 = 1,$$

$$\frac{11}{16} = 0,6875,$$

---

\* Эта дробь является одной из тех, которые наиболее близко подходят к значению квадратного корня из 23, причем ошибка меньше семи единиц в двадцатом десятичном знаке.

$$\begin{aligned}
 \frac{4}{5} &= 0,8, \\
 \frac{4}{9} &= 0,4444444444\ 4444444444\ 44\dots, \\
 \frac{22}{49} &= 0,4489795918\ 3673469387\ 75\dots, \\
 \frac{5}{13} &= 0,3846153846\ 1538461538\ 46\dots, \\
 \frac{7}{47} &= 0,1489361702\ 1276595744\ 68\dots, \\
 \frac{52}{59} &= 0,8813559322\ 0338983050\ 84\dots, \\
 \hline
 F &\approx 4.7958315233\ 1271954166\ 17
 \end{aligned}$$

Разность между этой суммой и верным значением заведомо меньше, чем пять единиц в последнем, двадцать втором, десятичном разряде, так что тем самым двадцать первых цифр не может измениться. Если провести вычисления для еще более далеких десятичных разрядов, то вместо последних двух цифр 17 получится 1893936...

Впрочем, каждый может заметить, даже если бы мы на это специально не указывали, что этот метод для превращения обыкновенных дробей в десятичные особенно предпочтителен в том случае, когда нужно найти много десятичных знаков; действительно, если достаточно немногих знаков, то в большинстве случаев столь же удобно применять простое деление или вычисление с логарифмами.

### 318

Так как тем самым превращение в десятичные дроби таких дробей, знаменатели которых составлены из нескольких простых чисел, уже сведено к тому случаю, когда знаменатель является простым числом или степенью простого числа, мы хотим добавить только еще кое-что относительно мантисс первых. Если знаменатель не содержит сомножителей 2 и 5, то мантисса и здесь будет состоять из периодов, так как и в этом случае в ряду 10, 100, 1000,... мы в конце концов дойдем до члена, который сравним с единицей по этому знаменателю, и одновременно показатель этого члена, который легко может быть определен на основании п. 92, будет указывать величину перио-

да, не зависящую от числителя, если он взаимно прост со знаменателем. Если же знаменатель имеет вид  $2^\alpha 5^\beta N$ , где  $N$  есть число взаимно простое с 10, и  $\alpha, \beta$  обозначают числа, хотя бы одно из которых не равно 0, то мантисса дроби только после первых  $\alpha$  или  $\beta$  цифр (в зависимости от того,  $\alpha$  или  $\beta$  больше) будет состоять из чистых периодов, которые в отношении своей длины будут совпадать с периодами дробей, знаменателем которых является  $N$ . Это легко выводится из того, что первая дробь разложима на две другие со знаменателями  $2^\alpha 5^\beta$  и  $N$ , первая из которых обрывается после  $\alpha$  или  $\beta$  цифр. Впрочем, относительно этого предмета мы могли бы добавить много других замечаний, особенно в отношении искусственных приемов, которые можно применять, чтобы по возможности быстро конструировать таблицу, подобную таблице 3, однако, ради краткости, мы откажемся здесь от этого, тем более, что многое относящееся сюда уже было указано как Робертсоном в ужецитированном сочинении, так и Б е р н у л л и («*Nouv. Mém. de l'Ac. de Berlin*», 1771, p. 273).

### Решение сравнения $x^2 \equiv A \pmod{m}$ методом исключения

#### 319

Вопрос о возможности сравнения  $x^2 \equiv A \pmod{m}$ , которое равносильно неопределенному уравнению  $x^2 = A + my$ , мы изложили в разделе IV (п. 146) так, что больше уже ничего не остается желать; относительно же самого нахождения неизвестных мы уже замечали выше (п. 152), что косвенные методы значительно предпочтительнее прямых. Если  $m$  есть простое число (к каковому случаю легко могут быть сведены остальные), то мы могли бы использовать для этой цели таблицу индексов 1 (согласно замечанию в п. 316, в соединении с таблицей 3), как мы подробнее показали в п. 60. Однако этот метод был бы ограничен пределами таблицы. По этой причине, как мы надеемся, следующий общий и удобный метод будет небезынтересным для любителей арифметики.

Прежде всего заметим, что достаточно иметь только те значения  $x$ , которые положительны и не больше чем  $m/2$ , ибо каждое другое значение сравнимо по модулю  $m$  либо с одним из самих этих значе-

ний, либо с одним из них, взятым с отрицательным знаком; но для такого значения  $x$  значение  $y$  обязательно будет содержаться между границами  $-\frac{A}{m}$  и  $\frac{1}{4}m - \frac{A}{m}$ . Метод, который непосредственно напрашивается, должен был бы состоять в том, что для отдельных, лежащих в этих границах значений  $y$ , совокупность которых мы обозначим через  $\Omega$ , вычисляется значение  $A + my$ , которое мы обозначим через  $V$ , и остаются только те значения, для которых  $V$  является квадратом. Если  $m$  — маленькое число (например, меньше чем 40), то этот способ настолько короток, что вряд ли требует упрощений; если же  $m$  велико, то при желании работа может быть сокращена посредством следующего метода исключения.

## 320

Пусть  $E$  — любое целое число, которое взаимно просто с  $m$  и меньше чем 2; далее, пусть все его различные (т. е. несравнимые по модулю  $E$ ) квадратичные невычеты суть  $a, b, c, \dots$ ; наконец, пусть корни сравнений

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c, \dots \pmod{E}$$

равны соответственно  $\alpha, \beta, \gamma, \dots$ , и все они положительны и меньше чем  $E$ , что мы имеем право предполагать. Если теперь придать  $y$  значение, которое сравнимо с одним из чисел  $\alpha, \beta, \gamma, \dots$  по модулю  $E$ , то получающееся при этом значение  $V = A + my$  будет сравнимо с одним из чисел  $a, b, c, \dots$  и потому будет невычетом по модулю  $E$ ; поэтому оно не может быть квадратом. Отсюда вытекает, что из  $\Omega$  тотчас же могут быть исключены как непригодные все числа, которые содержатся в формах  $Et + \alpha, Et + \beta, Et + \gamma, \dots$ , и будет достаточно произвести испытание остальных чисел, совокупность которых мы обозначим через  $\Omega'$ . При этой операции числу  $E$  можно дать название исключателя.

Если же взять в качестве исключателя другое подходящее число  $E'$ , то мы совершенно аналогичным образом найдем столько чисел  $\alpha', \beta', \gamma', \dots$ , сколько имеется различных квадратичных невычетов, с которыми  $y$  не может быть сравнимо по модулю  $E'$ . Поэтому из  $\Omega'$  снова можно будет выбросить все числа, содержа-

щиеся в формах  $E't + \alpha'$ ,  $E't + \beta'$ ,  $E't + \gamma'$ , ... Таким же образом исключение можно продолжать и дальше, применяя все новые и новые исключатели, до тех пор, пока количество чисел в  $\Omega$  не уменьшится настолько, что окажется не более трудно непосредственно испытать оставшиеся числа, чем применять новые исключения.

**Пример.** Если дано уравнение  $x^2 = 22 + 97y$ , то границы значений  $y$  равны  $-22/97$  и  $24\frac{1}{4} - \frac{22}{97}$ , так что  $\Omega$  охватывает числа 1, 2, 3, ..., 24 (ибо непригодность числа 0 непосредственно ясна). Для  $E = 3$  получается единственный невычет  $a = 2$ ; отсюда  $\alpha = 1$ ; поэтому из  $\Omega$  исключаются все числа вида  $3t + 1$ ; количество оставшихся чисел  $\Omega'$  равно 16. Точно так же для  $E = 4$  получается  $a = 2$ ,  $b = 3$ , откуда  $\alpha = 0$ ,  $\beta = 1$ ; поэтому отбрасываются все числа вида  $4t$  и  $4t + 1$ , и остаются следующие восемь: 2, 3, 6, 11, 14, 15, 18, 23. Точно так же для  $E = 5$  мы находим, что исключаются числа вида  $5t$  и  $5t + 3$ ; таким образом, остаются числа 2, 6, 11, 14. Исключатель 6 устранил бы числа вида  $6t + 1$  и  $6t + 4$ ; однако эти числа (которые совпадают с числами вида  $3t + 1$ ) уже отброшены. Исключатель 7 устраняет числа вида  $7t + 2$ ,  $7t + 3$ ,  $7t + 5$  и оставляет следующие: 6, 11, 14. Если подставить их вместо  $y$ , то получается  $V = 604, 1089, 1380$ ; из этих значений только второе является квадратом. Для него  $x = \pm 33$ .

### 321

Так как производимая при помощи исключателя  $E$  операция исключает из значений  $V$ , соответствующих значениям  $y$  из  $\Omega$ , все те значения, которые являются квадратичными невычетами по модулю  $E$ , а вычеты по этому числу оставляет неприкосновенными, то легко видеть, что применение  $E$  и  $2E$  ничем не отличается, если  $E$  нечетно, так как в этом случае  $E$  и  $2E$  имеют одни и те же вычеты и невычеты. Отсюда вытекает, что если в качестве исключателей использовать последовательно числа 3, 5, 7, ..., то четные числа, не делящиеся на 4, именно, 6, 10, 14, ... должны пропускаться как ненужные. Далее, очевидно, что дважды произ-

веденная операция при помощи исключателей  $E, E'$  устраняет все те значения  $V$ , которые являются невычетами либо обоих чисел  $E, E'$ , либо по крайней мере одного из них, в то время как значения, являющиеся вычетами обоих этих чисел, сохраняются. Но так как в случае, когда  $E$  и  $E'$  не имеют общих делителей, все устраненные числа являются невычетами, а все оставшиеся — вычетами по модулю  $EE'$ , то ясно, что в этом случае применение исключателя  $EE'$  приводит в точности к тому же, что и применение  $E$  и  $E'$ , и потому применять  $EE'$  после  $E$  и  $E'$  уже не нужно. Таким образом, мы можем отбросить все те исключатели, которые могут быть разложены на два взаимно простых сомножителя, и ограничиться теми, которые являются либо (не входящими в  $m$ ) простыми числами, либо степенями простых чисел. Наконец, ясно, что после применения исключателя  $p^\mu$ , являющегося степенью простого числа  $p$ , исключатели  $p$  и  $p^\nu$ , где  $\nu < \mu$ , уже становятся излишними; действительно, так как  $p^\mu$  оставляет среди значений  $V$  только вычеты по себе самому, то тем более не могут остаться невычеты по модулю  $p$  или по модулю более низкой чем  $p^\mu$  степени  $p^\nu$ . Если же исключатель  $p$  или  $p^\nu$  уже был применен до  $p^\mu$ , то последний, очевидно, может устранить только те значения  $V$ , которые одновременно являются вычетами по модулю  $p$  (или  $p^\nu$ ) и невычетами по модулю  $p^\mu$ ; поэтому достаточно брать в качестве  $a, b, c, \dots$  только такие вычеты числа  $p^\mu$ .

## 322

*Отыскание чисел  $\alpha, \beta, \gamma, \dots$ , которые соответствуют некоторому заданному исключателю  $E$ , может быть значительно сокращено благодаря следующим замечаниям. Пусть  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  суть корни сравнений  $my \equiv a, my \equiv b, my \equiv c, \dots \pmod{E}$ , и  $k$  — корень сравнения  $my \equiv -A$ ; тогда, очевидно,  $\alpha \equiv \mathfrak{A} + k, \beta \equiv \mathfrak{B} + k, \gamma \equiv \mathfrak{C} + k, \dots$  Если бы теперь нам действительно нужно было находить  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  посредством решения указанных сравнений, то этот путь определения  $\alpha, \beta, \gamma, \dots$  был бы во всяком случае не короче того, который мы указали выше; однако решать указанные сравнения вовсе не обязательно. Именно, если, сначала,  $E$  является простым числом,*



и  $t$  есть квадратичный вычет по модулю  $E$ , то из п. 98 вытекает, что  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$ , являющиеся значениями выражений  $a/t, b/t, c/t, \dots \pmod{E}$ , будут различными невычетами по модулю  $E$ , и потому в точности совпадают с  $\alpha, \beta, \gamma, \dots$ , если не принимать во внимание порядок их расположения, который здесь не важен; если же при сохранении остальных предположений  $t$  есть невычет по модулю  $E$ , то числа,  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  будут совпадать со всеми квадратичными вычетами (кроме 0). Если  $E$  есть квадрат (нечетного) простого числа скажем,  $E = p^2$ , и если  $p$  уже было использовано в качестве исключателя, то, согласно предыдущему пункту, в качестве  $a, b, c, \dots$  достаточно брать только те невычеты по модулю  $p^2$ , которые являются вычетами по модулю  $p$ , т. е. числа  $p, 2p, 3p, \dots, p^2 - p$  (именно, все числа, меньшие чем  $p^2$ , кроме 0, которые делятся на  $p$ ); но из этого легко видеть, что в качестве  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  должны получиться эти же самые числа, лишь расположенные в другом порядке. Аналогично, если после применения исключателей  $p$  и  $p^2$  мы положим  $E = p^3$ , то будет достаточно брать в качестве  $a, b, c, \dots$  произведения отдельных невычетов по модулю  $p$  на  $p^2$ , и  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  окажутся либо этими же самыми числами, либо произведениями числа  $p$  на отдельные вычеты по модулю  $p$  (за исключением 0), в зависимости от того, является ли  $t$  вычетом или невычетом по модулю  $p$ . Вообще, если взять в качестве  $E$  любую степень простого числа, скажем,  $p^\mu$ , после того как все более низкие степени уже были использованы, то в качестве  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  получатся произведения числа  $p^{\mu-1}$  либо на все числа, которые меньше  $p$  (0 все время исключается), в случае, когда  $\mu$  четно, либо на все меньшие чем  $p$  невычеты по модулю  $p$ , в случае, когда  $\mu$  нечетно и  $t \not\equiv 1 \pmod{p}$ , либо на все вычеты, если  $t \equiv 1 \pmod{p}$ . Если  $E = 4$  и потому  $a = 2, b = 3$ , то в качестве  $\mathfrak{A}, \mathfrak{B}$  мы получаем либо 2 и 3, либо 2 и 1, в зависимости от того, имеет ли место  $t \equiv 1$  или  $\equiv 3 \pmod{4}$ . Если после применения исключателя 4 мы положим  $E = 8$ , то получим  $\alpha = 5$ , откуда  $\mathfrak{A} = 5, 7, 1, 3$ , когда соответственно  $t \equiv 1, 3, 5, 7 \pmod{8}$ . Вообще же, если  $E$  есть любая более высокая степень числа 2, скажем,  $E = 2^\mu$ , то после того как более низкие степени числа 2 уже использованы, нужно положить  $a = 2^{\mu-1}, b = 3 \cdot 2^{\mu-2}$ , если  $\mu$  четно, откуда полу-

чается  $\mathfrak{A} = 2^{\mu-1}$ ,  $\mathfrak{B} = 3 \cdot 2^{\mu-2}$  или  $= 2^{\mu-2}$ , в зависимости от того, будет ли  $m \equiv 1$  или  $\equiv 3$ ; если же  $\mu$  нечетно, то нужно положить  $a = 5 \cdot 2^{\mu-3}$ , откуда  $\mathfrak{A}$  получится равным произведению числа  $2^{\mu-3}$  на одно из чисел 5, 7, 1 или 3, смотря по тому, будет ли  $m \equiv 1$ ,  $\equiv 3$ ,  $\equiv 5$  или  $\equiv 7 \pmod{8}$ .

Впрочем, искусные математики легко придумают аппарат, при помощи которого непригодные значения  $y$  будут отбрасываться *механически*, после того как числа  $\alpha, \beta, \gamma, \dots$  будут найдены для достаточного количества исключателей; однако для сокращения работы мы не будем здесь останавливаться на этом, так же, как и на других специальных приемах.

### Решение неопределенного уравнения $mx^2 + ny^2 = A$ методом исключения

323

В разделе V мы указали общий метод для отыскания всех представлений заданного числа  $A$  двойничной формой  $mx^2 + ny^2$ , или, другими словами, решения неопределенного уравнения  $mx^2 + ny^2 = A$ , который не оставляет желать в отношении краткости ничего лучшего, если мы уже знаем все значения выражения  $\sqrt{-mn}$  по самому модулю  $A$  и по модулю, получающемуся из  $A$  делением на его квадратные сомножители; однако для того случая, когда  $mn$  положительно, мы изложим сейчас метод, который на много удобнее только что упомянутого метода, если для последнего еще надо заранее вычислять указанные значения. При этом мы предположим, что числа  $m, n$  и  $A$  положительны и попарно взаимно просты, так как остальные случаи легко могут быть сведены к этому. Кроме того, достаточно, очевидно, искать только положительные значения  $x, y$ , так как остальные получаются из них всевозможными изменениями знаков.

Ясно, что  $x$  должен обладать тем свойством, что выражение  $(A - mx^2)/n$ , которое мы будем коротко обозначать через  $V$ , положительно, является целым и представляет собой квадрат. Первое условие требует, чтобы  $x$  был не больше чем  $\sqrt{A/m}$ ; второе

условие выполняется само собой, если  $n = 1$ , в противном же случае оно требует, чтобы значение выражения  $\frac{A}{m} \pmod{n}$  было квадратичным вычетом по модулю  $n$ ; и если мы обозначим все различные значения выражения  $\sqrt{\frac{A}{m}} \pmod{n}$  через  $\pm r, \pm r', \dots$ , то значения  $x$  должны будут содержаться в одной из форм  $nt + r, nt - r, nt + r', \dots$ . Поэтому проще всего было бы подставлять вместо  $x$  все не превосходящие границы  $\sqrt{A/m}$  числа такого вида, совокупность которых мы обозначим через  $\Omega$ , и оставлять только те, для которых  $V$  является квадратом. В следующем пункте мы покажем, как этот способ можно при желании сократить.

## 324

Метод исключений, при помощи которого мы этого добьемся, состоит, так же, как и в предыдущем исследовании, в том, что берутся некоторые числа, которые мы и здесь будем называть исключениями, затем исследуется, для каких значений  $x$  значения  $V$  будут квадратичными невычетами по этим исключениям, и такие значения  $x$  из  $\Omega$  выбрасываются. Из рассуждений, которые совершенно аналогичны изложенным в п. 321, вытекает, что нужно использовать только те исключения, которые являются простыми числами или степенями простых чисел, и для исключения второго типа из значений  $V$  нужно отбрасывать только те невычеты этого исключения, которые являются вычетами всех более низких степеней того же простого числа, если для них исключение уже проведено.

Итак, пусть исключатель  $E$  равен  $p^\mu$  (включая и тот случай, когда  $\mu = 1$ ), где  $p$  есть не входящее в  $m$  простое число; предположим, что  $p^\nu$  есть наивысшая степень этого простого числа, на которую делится  $n^*$ . Пусть, далее,  $a, b, c, \dots$  суть квадратичные невычеты по модулю  $E$  (причем все, если  $\mu = 1$ , и лишь те, которые являются вычетами по более низким степеням, если  $\mu > 1$ ). Если вычислить корни сравнений

$$tz \equiv A - na, \quad tz \equiv A - nb, \quad tz \equiv A - nc, \dots \pmod{Ep^\nu = p^{\mu+\nu}},$$

---

\* Ради краткости мы объединяем оба случая, когда  $n$  делится и не делится на  $p$ ; в последнем случае надо положить  $\nu = 0$ .

которые мы обозначим через  $\alpha, \beta, \gamma, \dots$ , то легко получится, что если для некоторого значения  $x$  имеет место  $x^2 \equiv \alpha \pmod{Ep^v}$ , то соответствующее значение  $V$  будет  $\equiv a \pmod{E}$ , т. е. будет невычетом по модулю  $E$ , и аналогично обстоит дело для  $\beta, \gamma, \dots$ . Обратно, столь же очевидно, что если некоторое значение  $x$  приводит к сравнению  $V \equiv a \pmod{E}$ , то для этого значения будет  $x^2 \equiv \alpha \pmod{Ep^v}$ , и потому все значения  $x$ , для которых  $x^2$  несравнимо по модулю  $Ep^v$  ни с одним из чисел  $\alpha, \beta, \gamma, \dots$ , приводят к таким значениям  $V$ , которые несравнимы ни с одним из чисел  $a, b, c, \dots$  по модулю  $E$ . Выберем теперь из чисел  $\alpha, \beta, \gamma, \dots$  все квадратичные вычеты по модулю  $Ep^v$ , которые обозначим через  $g, g', g'', \dots$ , и найдем значения выражений  $\sqrt{g}, \sqrt{g'}, \sqrt{g''}, \dots \pmod{Ep^v}$ , которые обозначим через  $\pm h, \pm h', \pm h'', \dots$ . Тогда ясно, что все числа вида  $Ep^v t \pm h, Ep^v t \pm h', Ep^v t \pm h'', \dots$  заведомо могут быть выброшены из  $\Omega$ , и что ни одному из значений  $x$ , еще оставшемуся в  $\Omega$  после этого исключения, не может отвечать значение  $V$ , содержащееся в формах  $Eu + a, Eu + b, Eu + c, \dots$ . Впрочем, такие значения  $V$ , очевидно, уже и сами по себе не могут получиться ни из каких значений  $x$ , если среди чисел  $\alpha, \beta, \gamma, \dots$  нет квадратичных вычетов по модулю  $Ep^v$ , и потому в этом случае применение числа  $E$  в качестве исключателя ничего не дает.

Мы можем применять сколько угодно исключателей, и тем самым все более и более сужать круг чисел, остающихся в  $\Omega$ .

Теперь убедимся, что простые числа, которые входят в  $m$ , или степени таких простых чисел нельзя использовать в качестве исключателей. Если  $B$  есть значение выражения  $\frac{A}{n} \pmod{m}$ , то получается, что какое бы значение для  $x$  ни брать,  $V$  будет всегда сравнимо с  $B$  по модулю  $m$ , и что тем самым для разрешимости заданного уравнения необходимо, чтобы  $B$  было квадратичным вычетом по модулю  $m$ . Поэтому, если обозначить через  $p$  какой-нибудь нечетный простой делитель числа  $m$ , который по предположению не входит в  $n$  и  $A$ , а, значит, и в  $B$ , то  $V$  для любого значения  $x$  будет вычетом по модулю  $p$ , а потому и по любой степени числа  $p$ ; следовательно, число  $p$  и его степени не могут

служить в качестве исключателей. Если  $m$  делится на 8, то по совершенно аналогичной причине для разрешимости заданного уравнения необходимо, чтобы имело место  $B \equiv 1 \pmod{8}$ , вследствие чего для любого значения  $x$  будет  $V \equiv 1 \pmod{8}$ , так что степени числа 2 не годятся в качестве исключателей. Если же  $m$  делится на 4, но не делится на 8, то по аналогичной причине должно быть  $B \equiv 1 \pmod{4}$ , и значение выражения  $\frac{A}{n} \pmod{8}$  будет равно 1 или 5; обозначим его через  $C$ . Без труда можно увидеть, что для четного значения  $x$  будет  $V \equiv C$ , а для нечетного будет  $V \equiv C + 4 \pmod{8}$ , откуда вытекает, что нужно отбросить четные значения, когда  $C = 5$ , и нечетные, когда  $C = 1$ . Если, наконец,  $m$  делится на 2, но не делится на 4, то пусть, как и раньше,  $C$  будет значением выражения  $\frac{A}{n} \pmod{8}$ , которое равно 1, 3, 5 или 7, и  $D$  — значение выражения  $\frac{m}{2n} \pmod{4}$ , равное 1 или 3. Так как теперь значение  $V$ , очевидно, всегда  $\equiv C - 2Dx^2 \pmod{8}$ , и потому для четного  $x$  оно  $\equiv C$ , а для нечетного  $\equiv C - 2D$ , то отсюда без труда выводится, что нужно отбросить все нечетные значения  $x$ , если  $C = 1$ , все четные, если  $C = 3$  и  $D = 1$  или  $C = 7$  и  $D = 3$ , и что для всех остальных значений  $V \equiv 1 \pmod{8}$ , т. е.  $V$  является вычетом по каждой степени числа 2; в остальных же случаях, именно, когда  $C = 5$ , или  $C = 3$  и  $D = 3$ , или  $C = 7$  и  $D = 1$ , будет иметь  $V \equiv 3, \equiv 5$  или  $\equiv 7 \pmod{8}$ , независимо от того, четно  $x$  или нечетно, откуда следует, что в этих случаях заданное уравнение вообще не имеет решений.

Так как точно так же, как мы научились здесь находить посредством исключений значения  $x$ , можно, с необходимыми изменениями находить и значения  $y$ , то метод исключения для решения поставленного вопроса всегда можно применять двояким образом (за исключением случая  $m = n = 1$ , когда оба способа совпадают), и в большинстве случаев предпочтительнее тот путь, при котором  $\Omega$  содержит меньшее количество членов, что легко можно узнать заранее. Наконец, вряд ли даже нужно указывать на то, что если после нескольких исключений из  $\Omega$  оказываются выброшенными все числа, — то это можно рассматривать как верный признак неразрешимости заданного уравнения.

**Пример.** Пусть дано уравнение  $3x^2 + 455y^2 = 10\,857\,362$ , которое мы хотим решить двумя способами: *сначала* ища значения  $x$ , а *затем* — значения  $y$ . Граница первых значений в этом случае равна числу  $\sqrt{10\,857\,362/3}$ , которое расположено между 1902 и 1903; значение выражения  $\frac{A}{3} \pmod{455}$  равно 354, и значения выражения  $\sqrt{354} \pmod{455}$  суть  $\pm 82, \pm 152, \pm 173, \pm 212$ . Поэтому  $\Omega$  состоит из следующих 33 чисел: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. Число 3 в данном случае в качестве исключателя брать нельзя, так как оно входит в  $m$ . Для исключателя 4 мы имеем  $a = 2, b = 3$ , откуда  $\alpha = 0, \beta = 3; g = 0$ , и в качестве значений выражения  $\sqrt{g} \pmod{4}$  получаются числа 0 и 2; отсюда следует, что все числа вида  $4t$  и  $4t + 2$ , т. е. все четные числа, из  $\Omega$  выбрасываются; совокупность оставшихся (шестнадцати) чисел обозначим через  $\Omega'$ . Для числа  $E = 5$ , которое входит в  $n$ , мы получаем в качестве корней сравнений  $mz \equiv A - 2n$  и  $mz \equiv A - 3n \pmod{25}$  значения 9 и 24, которые оба являются вычетами по модулю 25, причем значения выражений  $\sqrt{9}$  и  $\sqrt{24} \pmod{25}$  суть  $\pm 3, \pm 7$ ; после отбрасывания из  $\Omega'$  всех чисел вида  $25t \pm 3, 25t \pm 7$  остается совокупность из следующих десяти чисел: 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577 обозначим ее через  $\Omega''$ . Для  $E = 7$  мы в качестве корней сравнений  $mz \equiv A - 3n, mz \equiv A - 5n, mz \equiv A - 6n \pmod{49}$  имеем значения 32, 39, 18, которые все являются вычетами по модулю 49, а в качестве значений выражений  $\sqrt{32}, \sqrt{39}, \sqrt{18} \pmod{49}$  числа  $\pm 9, \pm 23, \pm 19$ ; если выбросить из  $\Omega''$  числа вида  $49t \pm 9, 49t \pm 23, 49t \pm 19$ , то останется следующая совокупность  $\Omega'''$  из пяти чисел: 537, 737, 1083, 1213, 1517. Для  $E = 8$  мы получаем  $a = 5$ , и потому  $\alpha = 5$ , т. е.  $\alpha$  есть невычет по модулю 8; поэтому число 8 в качестве исключателя применять нельзя. Число 9 не годится по той же причине, что и 3. Для  $E = 11$  числа  $a, b, \dots$  будут соответственно равны 2, 6, 7, 8, 10, далее,  $v = 0$ , и потому  $\alpha, \beta, \dots = 8, 10, 5, 0, 1$ ; из этих чисел вычетами по модулю 11 будут только три, именно, 0, 1, 5; из этого следует, что из  $\Omega'''$  нужно выбросить числа вида

$11t$ ,  $11t \pm 1$ ,  $11t \pm 5$ , так что останутся лишь числа 537, 1083, 1213. Если эти числа испробовать, то для  $V$  соответственно получатся значения 21 961, 16 129, 14 161, из которых квадратами являются только второе и третье. Поэтому заданное уравнение обладает двумя решениями в положительных  $x$ ,  $y$ , именно,  $x = 1083$ ,  $y = 127$  и  $x = 1213$ ,  $y = 119$ .

*Второе.* Если мы хотим найти посредством исключений другое из двух неизвестных того же уравнения, то целесообразно, поменяв местами  $x$  и  $y$ , представить это уравнение в форме  $455x^2 + 3y^2 = 10\,857\,362$ , чтобы можно было сохранить все обозначения пп. 323, 324. Граница значений  $x$  оказывается здесь между 154 и 155; значение выражения  $\frac{A}{m} \pmod{n}$  равно 1, значения  $\sqrt{1} \pmod{3}$  суть  $+1$  и  $-1$ . Поэтому  $\Omega$  содержит все числа вида  $3t + 1$  и  $3t - 1$ , т. е. все числа, не делящиеся на 3, до 154 включительно; количество их равно 103. Если, однако, применить указанные выше принципы, то мы найдем, что для исключателей 3; 4; 9; 11; 17; 19; 23 из  $\Omega$  выбрасываются соответственно числа следующего вида:  $9t \pm 4$ ;  $4t$ ,  $4t \pm 2$ , т. е. все четные числа;  $27t \pm 1$ ,  $27t \pm 10$ ;  $11t$ ,  $11t \pm 1$ ,  $11t \pm 3$ ;  $17t \pm 3$ ,  $17t \pm 4$ ,  $17t \pm 5$ ,  $17t \pm 7$ ;  $19t \pm 2$ ,  $19t \pm 3$ ,  $19t \pm 8$ ,  $19t \pm 9$ ;  $23t$ ,  $23t \pm 1$ ,  $23t \pm 5$ ,  $23t \pm 7$ ,  $23t \pm 9$ ,  $23t \pm 10$ . После этого остаются лишь числа 119, 127, для которых  $V$  оказывается квадратом и которые приводят к тем же решениям, что мы получили выше.

## 326

*Указанный только что метод* уже и сам по себе настолько удобен, что почти не оставляет желать ничего лучшего; однако он может быть еще значительно сокращен при помощи ряда специальных приемов, которых мы здесь лишь коротко коснемся. При этом мы ограничимся тем случаем, когда исключатель есть нечетное простое число, не входящее в  $A$ , или степень такого простого числа, так как остальные случаи либо сводятся к этому, либо могут быть рассмотрены аналогичным образом. Если мы предположим сначала, что исключатель  $E = p$  есть не входящее в  $m$ ,  $n$  простое число, и что значения выражений  $\frac{A}{m}$ ,  $-\frac{pa}{m}$ ,  $-\frac{pb}{m}$ ,



$-\frac{nc}{m}, \dots (\bmod p)$  суть соответственно  $k, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$ , то числа  $\alpha, \beta, \gamma, \dots$  мы найдем при помощи сравнений  $\alpha \equiv k + \mathfrak{A}, \beta \equiv k + \mathfrak{B}, \gamma \equiv k + \mathfrak{C}, \dots (\bmod p)$ . Однако числа  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$  можно найти и не решая сравнений, посредством специального приема, который совершенно аналогичен приему, использованному в п. 322, причем эти числа будут совпадать либо со всеми невычетами, либо со всеми вычетами (кроме 0) по модулю  $p$ , в зависимости от того, вычетом или невычетом по модулю  $p$  будет значение выражения  $-\frac{m}{n} (\bmod p)$ , или, что то же самое, число  $-mn$ . Так, во втором примере предыдущего пункта для  $E = 17$  имеем  $k = 7; -mn = -1365 \equiv 12$ , т. е.  $-mn$  невычет по модулю 17; поэтому числа  $\mathfrak{A}, \mathfrak{B}, \dots$  равны 1, 2, 4, 8, 9, 13, 15, 16, а числа  $\alpha, \beta, \dots$  равны соответственно 8, 9, 11, 15, 16, 3, 5, 6; из них вычетами являются 8, 9, 11, 15, 16, поэтому  $\pm h, \pm h', \dots$  будут здесь равны  $\pm 5, \pm 3, \pm 7, \pm 4$ . Те, которым часто нужно решать подобный вопрос, значительно облегчат себе дело, если будут вычислять значения  $h, h', \dots$ , соответствующие отдельным значениям  $k$  (1, 2, 3,  $\dots, p-1$ ), при каждом из двух предположений (именно, что  $-mn$  является или вычетом, или невычетом по модулю  $p$ ) сразу для нескольких значений  $p$ . Заметим еще, что количество чисел  $h, -h, h', \dots$  всегда равно  $(p-1)/2$ , если оба числа  $k$  и  $-mn$  являются одновременно либо вычетами, либо невычетами по модулю  $p$ ; далее, это количество равно  $(p-3)/2$ , если первое число есть вычет, а второе невычет, и равно  $(p+1)/2$ , если первое число невычет, а второе вычет; однако доказательство этой теоремы мы должны опустить, чтобы не быть слишком пространными.

Что же касается *второго случая*, именно, когда  $E$  есть либо входящее в  $n$  простое число, либо степень (нечетного) простого числа, безразлично, входящего в  $n$  или нет, то он может быть разобран еще проще. Положим, сохраняя все обозначения п. 324,  $n = n'p^\nu$ , где  $n'$  не делится на  $p$ . Числа  $a, b, c, \dots$  будут произведениями числа  $p^{\mu-1}$  либо на все числа, меньшие чем  $p$  (кроме 0), либо на все меньшие чем  $p$  невычеты по модулю  $p$ , в зависимости от того, четно  $\mu$  или нечетно; будем записывать эти числа в виде  $ur^{\mu-1}$ . Если  $k$  есть значение выражения  $\frac{A}{m} (\bmod p^{\mu+\nu})$ , то  $k$  не делит-



ся на  $p$ , потому что по предположению на  $p$  не делится  $A$ ; далее, ясно, что все числа  $\alpha, \beta, \gamma, \dots$  будут сравнимы с  $k$  по модулю  $p$ , и потому  $p^\mu$  не произведет в  $\Omega$  никакого исключения, если  $kNp$ ; если же  $kRp$ , а потому и  $kRp^{\mu+\nu}$ , то пусть  $r$  будет (не делящимся на  $p$ ) значением выражения  $\sqrt{k} \pmod{p^{\mu+\nu}}$ , и  $e$  — значением выражения  $-\frac{n'}{2mr} \pmod{p}$ ; тогда  $\alpha \equiv r^2 + 2erap^\nu \pmod{p^{\mu+\nu}}$ , откуда легко видеть, что  $\alpha$  есть вычет по модулю  $p^{\mu+\nu}$ , и значения выражения  $\sqrt{\alpha} \pmod{p^{\mu+\nu}}$  суть  $\pm(r + eap^\nu)$ . Поэтому все значения  $h, h', h'', \dots$  будут представляться в виде  $r + uer^{\mu+\nu-1}$ . Наконец, мы легко заключаем отсюда, что числа  $h, h', h'', \dots$  получаются прибавлением числа  $r$  к произведениям числа  $p^{\mu+\nu-1}$  либо на все числа, меньшие чем  $p$  (кроме 0), в случае, когда  $\mu$  четно, либо на все невычеты по модулю  $p$ , не превосходящие той же границы, в случае, когда  $\mu$  нечетно и  $eRp$  (или, что то же самое, когда  $-2mrn'Rp$ ), либо на все вычеты (кроме 0), когда  $\mu$  нечетно и  $-2mrn'Np$ .

Впрочем, после того как для отдельных исключателей, которые мы захотим применить, числа  $h, h', h'', \dots$  будут найдены, само исключение можно будет производить также и чисто автоматически, в чем легко может убедиться всякий, имеющий в этих вещах некоторый опыт и потративший некоторые усилия.

Наконец, мы должны заметить, что каждое уравнение  $ax^2 + 2bxy + cy^2 = M$ , у которого  $b^2 - ac$  равно отрицательному числу  $-D$ , легко может быть сведено к виду, рассмотренному ранее. Именно, если обозначить наибольший общий делитель чисел  $a, b$  через  $m$  и положить

$$a = ma', \quad b = mb',$$

$$\frac{D}{m} = a'c - mb'^2 = n, \quad a'x + b'y = x',$$

то указанное уравнение, очевидно, будет эквивалентно уравнению  $mx'^2 + ny^2 = a'M$ , которое можно решить при помощи указанных выше правил. При этом из решений последнего уравнения нужно оставить только те, у которых  $x' - b'y$  делится на  $a'$ , т. е. из которых получаются целые значения для  $x$ .

## Другой метод решения сравнения $x^2 \equiv A$ в случае, когда $A$ отрицательно

327

В то время как изложенный в разделе V прямой метод решения уравнения  $ax^2 + 2bxy + cy^2 = M$  предполагает известными значения выражения  $\sqrt{b^2 - ac} \pmod{M}$ , только что изложенный косвенный метод в случае, когда  $b^2 - ac$  отрицательно, дает, наоборот, очень простой метод для отыскания этих значений, который, особенно для очень большого значения  $M$ , намного предпочтительней метода, содержащегося в п. 322 и сл. Мы будем предполагать, что число  $M$  простое, или по крайней мере, что если оно составное, то его сомножители еще неизвестны; действительно, если бы мы знали, что простое число  $p$  входит в  $M$ , и что  $M = p^\mu M'$ , где  $M'$  уже не содержит сомножителя  $p$ , то нам было бы намного удобнее найти значения выражения  $\sqrt{b^2 - ac}$  отдельно для модулей  $p^\mu$  и  $M'$  (причем для первого из значений для модуля  $p$ , п. 101), и, уже комбинируя их, получить значения по модулю  $M$  (п. 105).

Итак, отыскиваются все значения выражения  $\sqrt{-D} \pmod{M}$ , где  $D$  и  $M$  предполагаются положительными числами, причем  $M$  содержится в форме делителей выражения  $x^2 + D$  (пп. 147 и сл.), так как иначе заранее было бы известно, что никакие числа не могут быть значениями данного выражения. Обозначим искомые значения, которые всегда разбиваются на пары противоположных одно другому, через  $\pm r, \pm r', \pm r'', \dots$ , и положим  $D + r^2 = Mh$ ,  $D + r'^2 = Mh'$ ,  $D + r''^2 = Mh'' \dots$ ; далее, обозначим классы, к которым принадлежат формы  $(M, r, h), (M, -r, h), (M, r', h'), (M, -r', h'), (M, r'', h''), (M, -r'', h''), \dots$  соответственно через  $\mathfrak{E}, -\mathfrak{E}, \mathfrak{E}', -\mathfrak{E}', \mathfrak{E}'', -\mathfrak{E}'', \dots$ , а их совокупность через  $\mathfrak{G}$ . Правда, эти классы, вообще говоря, следует рассматривать как неизвестные, однако ясно, во-первых, что все они положительны и собственно примитивны, и, во-вторых, что все они принадлежат одному и тому же роду, характер которого легко может быть определен по свойствам числа  $M$ , т. е. по его отношениям к отдельным простым делителям числа  $D$  (и, кроме того, иногда также и к числам 4 и 8; п. 230). Так как по предположению  $M$  содержится в форме делителей выражения

$x^2 + D$ , мы можем заранее быть уверены, что этому характеру обязательно соответствует положительный собственно примитивный род форм с определителем  $-D$ , даже если выражение  $\sqrt{-D} \pmod{M}$  и вовсе не имеет значений; так как теперь этот род нам известен, можно найти все содержащиеся в нем классы; обозначим их через  $C, C', C'', \dots$ , а их совокупность через  $G$ . Тогда ясно, что каждый класс  $\mathfrak{C}, -\mathfrak{C}, \dots$  должен совпадать с некоторым классом из  $G$ ; при этом может случиться, что несколько классов из  $\mathfrak{G}$  совпадают между собой, а потому совпадают с одним и тем же классом из  $G$ , а если  $G$  содержит только один класс, то с ним будут совпадать все классы из  $\mathfrak{G}$ . Поэтому если из классов  $C, C', C'', \dots$  выбрать, по одной из каждого, (простейшие) формы  $f, f', f'', \dots$ , то каждый класс из  $\mathfrak{G}$  будет содержать одну из этих форм. Если теперь  $ax^2 + 2bxy + cy^2$  есть форма, содержащаяся в классе  $\mathfrak{C}$ , то существует два принадлежащих значению  $r$  представления числа  $M$  этой формой, причем если одно из них есть  $x=t, y=n$ , то другое будет  $x=-t, y=-n$ ; лишь случай  $D=1$  составляет исключение, так как здесь имеется четыре представления (ср. п. 180).

Из этого мы заключаем, что если найти (изложенным выше косвенным методом) все представления числа  $M$  отдельными формами  $f, f', f'', \dots$  и определить затем все значения выражения  $\sqrt{-D} \pmod{M}$ , которым отдельные представления принадлежат (п. 154), то мы получим тем самым все значения этого выражения, причем каждое по два раза или, в случае  $D=1$ , по четыре раза; тем самым, задача решена. Если среди  $f, f', f'', \dots$  окажутся формы, которыми число  $M$  представлено быть не может, то это будет означать, что эти формы не принадлежат к  $\mathfrak{G}$  и потому должны быть отброшены; если же  $M$  не может быть представлено ни одной из указанных форм, то  $-D$  с необходимостью будет квадратичным невычетом по модулю  $M$ .

*Относительно этих операций мы сделаем еще следующие замечания.*

I. Под представлениями числа  $M$  формами  $f, f', \dots$ , которые мы здесь используем, понимаются лишь такие представления, у которых значения неизвестных взаимно просты; если же получаются еще и другие представления, у которых указанные значения имеют об-

щий делитель (что возможно только тогда, когда  $\mu^2$  входит в  $M$  и заведомо имеет место, если  $-DR \frac{M}{\mu^2}$ , то при исследовании этого вопроса их нужно просто отбрасывать, хотя в других вопросах они и могут играть роль.

II. При прочих равных условиях работа будет, очевидно, тем легче, чем меньше количество классов форм, и потому она будет всего короче, когда  $D$  равно одному из указанных в п. 303 шестидесятипяти чисел, для которых в отдельных родах имеется только по одному классу.

III. Так как каждые два представления вида  $x = m$ ,  $y = n$ ;  $x = -m$ ,  $y = -n$  принадлежат всегда одному и тому же значению, то, очевидно, достаточно рассматривать только такие представления, у которых  $y$  положительно. Различные представления такого типа всегда соответствуют уже различным значениям выражения  $\sqrt{-D} \pmod{M}$ , так что число всех различных значений равно числу всех, получающихся представлений такого рода (случай  $D = 1$ , когда первое число равно половине второго, снова составляет исключение).

IV. Поскольку как только мы узнаем одно из противоположных значений  $+r$ ,  $-r$ , нам тем самым становится известно и другое, мы можем еще несколько сократить наши операции. Если значение  $r$  было найдено из представления числа  $M$  формой из класса  $C$ , т. е. если  $\mathfrak{C} = C$ , то противоположное значение  $-r$  получается, очевидно, из представления той формой, которая содержится в классе, противоположном классу  $C$ , и потому отличном от него, если только  $C$  не является двусторонним классом. Отсюда следует, что если не все классы из  $G$  двусторонние, то из остальных нужно рассматривать только половину, именно, по одному классу из каждой двух противоположных, отбрасывая другой, так как из него, как мы уже знаем, без всяких вычислений получаются значения, противоположные тем, которые дает оставленный класс. Если же класс  $C$  двусторонний, то из него одновременно получаются оба значения  $r$  и  $-r$ ; именно, если в  $C$  выбрана двусторонняя форма  $ax^2 + 2bxy + cy^2$ , и значение  $r$  получается из представления  $x = m$ ,  $y = n$ , то значение  $-r$  получится из представления  $x = -m - \frac{2bn}{a}$ ,  $y = n$ .

V. В том случае, когда  $D = 1$ , имеется вообще только один класс, в качестве представителя которого можно считать выбранной форму  $x^2 + y^2$ . Если теперь значение  $r$  получается из представления  $x = m, y = n$ , то из представлений  $x = -m, y = -n$ ;  $x = -m, y = n$ ;  $x = m, y = -n$  будет получаться это же значение, а из представлений  $x = m, y = -n$ ;  $x = -m, y = n$ ;  $x = n, y = m$ ;  $x = -n, y = -m$  — противоположное значение  $-r$ . Поэтому из этих восьми представлений, которые дают только одно разложение, достаточно знать лишь одно представление, если только к значению, получающемуся из него, добавить еще противоположное значение.

VI. Согласно п. 155, значение выражения  $\sqrt{-D} \pmod{M}$ , которому принадлежит представление  $M = am^2 + 2bmn + cn^2$ , равно либо  $\mu(mb + nc) - \nu(ma + nb)$ , либо некоторому сравнимому с  $\mu(mb + nc) - \nu(ma + nb)$ , по модулю  $M$  числу, где  $\mu, \nu$  таковы, что  $\mu m + \nu n = 1$ . Если поэтому обозначить какое-нибудь из таких чисел через  $v$ , то будет иметь место

$$mv \equiv \mu m (mb + nc) - \nu (M - mnb - n^2c) \equiv (\mu m + \nu n) (mb + nc) \equiv \\ \equiv mc + nc \pmod{M}.$$

Отсюда вытекает, что  $v$  является значением выражения  $\frac{mb + nc}{m} \pmod{M}$ , и подобным же образом мы находим, что  $v$  есть значение выражения  $-\frac{ma + nb}{n} \pmod{M}$ . Эти формулы очень часто оказываются предпочтительнее тех, из которых они выведены.

328

Примеры. I. Найдем все значения выражения

$$\sqrt{-1365} \pmod{5\,428\,681 = M}.$$

Число  $M$  здесь  $\equiv 1, 1, 1, 6, 11 \pmod{4, 3, 5, 7, 13}$ , и потому содержится в форме делителей выражений  $x^2 + 1, x^2 + 3, x^2 - 5$  и в форме неделителей выражений  $x^2 + 7, x^2 - 13$ , т. е. содержится в форме делителей выражения  $x^2 + 1365$ ; характер рода, в котором находятся классы из  $\mathfrak{G}$ , есть 1, 4;  $R3$ ;  $R5$ ;  $N7$ .  $N13$ . В этом роде содержится только один класс, из

которого мы выбираем форму  $6x^2 + 6xy + 229y^2$ . Чтобы получить все представления этой формой числа  $M$ , мы положим  $2x + y = x'$ ; тогда получается уравнение  $3x'^2 + 455y^2 = 2M$ . Оно имеет четыре решения с положительными  $y$ , именно,  $y = 127$ ,  $x' = \pm 1083$ ;  $y = 119$ ,  $x' = \pm 1213$ . Отсюда получаются четыре решения с положительными  $y$  уравнения  $6x^2 + 6xy + 229y^2 = M$ , именно,

$$\begin{array}{c|c|c|c|c} x & 478 & -605 & 547 & -666 \\ y & 127 & 127 & 119 & 119 \end{array}.$$

Первое решение дает для  $v$  значение выражения  $\frac{30\,517}{478}$  или  $-\frac{3249}{127} \pmod{M}$ , откуда мы находим  $v = 2\,350\,978$ ; второе дает противоположное значение  $-2\,350\,978$ , третье — значение  $2\,600\,262$ , и четвертое решение — противоположное значение  $-2\,600\,262$ .

II. Если нужно найти значения выражения

$$\sqrt{-286} \pmod{4\,272\,943 = M},$$

то в качестве характера рода, в котором содержатся классы из  $\mathfrak{G}$ , мы получаем 1 и 7, 8;  $R_{11}$ ;  $R_{13}$ ; таким образом, этот род является главным родом, содержащим три класса, представителями которых служат формы  $(1, 0, 286)$ ,  $(14, 6, 23)$ ,  $(14, -6, 23)$ ; третью из них можно отбросить, так как она противоположна второй. Для формы  $x^2 + 286y^2$  мы находим два представления числа  $M$  с положительными  $y$ , именно,  $y = 103$ ,  $x = \pm 1113$ , из которых получаются следующие значения искомого выражения:  $1\,493\,445$ ,  $-1\,493\,445$ . Формой же  $(14, 6, 23)$  число  $M$  не представляется, откуда следует, что других значений, кроме двух уже найденных, не существует.

III. Если задано выражение  $\sqrt{-70} \pmod{997\,331}$ , то классы  $\mathfrak{G}$  должны содержаться в роде, характером которого является 3 и 5, 8;  $R_5$ ;  $N_7$ ; этот род содержит только один класс, представителем которого является форма  $(5, 0, 14)$ . Если мы, однако, произведем вычисления, то убедимся, что число  $997\,331$  формой  $(5, 0, 14)$  не представляется, вследствие чего  $-70$  является квадратичным невычетом этого числа.

## Два метода отличать составные числа от простых и находить сомножители составных чисел

329

То, что задача о том, как отличать составные числа от простых и разлагать первые на их простые сомножители принадлежит к важнейшим задачам всей арифметики и привлекала внимание как математиков древности, так и математиков нашего времени, настолько хорошо известно, что было бы излишним тратить здесь на это много слов. Однако, нужно отметить, что все известные до сих пор методы либо ограничиваются очень специальными случаями, либо настолько длинны и трудоемки, что даже для чисел, не выходящих за пределы таблиц, составленных заслуженными математиками, т. е. чисел, для которых особо искусные методы не нужны, они утомительны даже для опытных вычислителей, а для еще бóльших чисел почти совершенно неприменимы. И хотя вышеупомянутые таблицы, которые доступны всем и которые, как мы надеемся, скоро будут еще расширены, обычно оказываются достаточными, тем не менее опытные вычислители нередко сталкиваются с таким положением, когда умение разложить большое число на простые сомножители приносит им пользу, вполне компенсирующую большую затрату времени; кроме того, и интересы самой науки как таковой обязывают приложить все усилия к решению этой столь изящной и знаменитой проблемы. Именно поэтому мы не сомневаемся, что оба нижеследующих метода, в действительности и краткости которых мы убедились на долгом опыте, не должны оказаться бесполезными для любителей арифметики. Впрочем, по самой природе этого вопроса любой метод становится все более трудоемким по мере того, как числа, к которым он применяется, становятся все бóльшими и бóльшими; однако в случае обоих приводимых ниже методов трудности нарастают очень медленно, и числа, состоящие из семи, восьми и даже большего числа цифр, особенно при применении второго метода, всегда исследуются с такой быстротой, которую по справедливости следует считать достаточной для столь больших чисел, работа с которыми при помощи известных ранее методов представляла бы невыносимый труд даже для неутомимых вычислителей.

Прежде чем применять нижеследующие методы, всегда бывает целесообразно исследовать предварительно делимость заданного числа на маленькие простые числа, например, на 2, 3, 5, 7, ... до 19 или еще дальше, не только потому, что такие числа, в случае, если они являются делителями, гораздо проще обнаружить непосредственным делением, нежели применять к ним тонкие искусственные методы, но и потому, что если ни одно из делений не выполняется без остатка, получающиеся остатки с большой выгодой могут быть использованы при применении второго метода. Если, например, нужно разложить на множители число 314 159 265, то деление на 3 оказывается выполнимым дважды, а также оказывается выполнимым деление на 5 и 7, так что мы получаем  $314\ 159\ 265 = 9 \cdot 5 \cdot 7 \cdot 997\ 331$ , и нам достаточно подвергнуть более подробному исследованию только число 997 331, которое на 11, 13, 17, 19 не делится. Аналогично, если задано число 43 439 448, то устраняется сомножитель 8, и более тонкие методы применяются уже по отношению к числу 5 428 681.

## 330

*В основе первого метода лежит теорема, что каждое положительное или отрицательное число, которое является квадратичным вычетом по некоторому другому числу  $M$ , будет квадратичным вычетом также и по всякому делителю числа  $M$ .* Известно, что если  $M$  не делится ни на какое простое число, меньшее чем  $\sqrt{M}$ , то  $M$  обязательно является простым числом; кроме того, если все простые числа, входящие в  $M$  и не превосходящие этой границы, суть  $p, q, \dots$ , то число  $M$  делится либо только на эти простые числа (и их степени), либо, быть может, еще только на одно простое число, которое больше чем  $\sqrt{M}$  и которое можно найти, поделив  $M$  на  $p, q, \dots$ . Поэтому, если обозначить через  $\Omega$  совокупность всех простых чисел, меньших чем  $\sqrt{M}$  (за исключением тех, в неделимости на которые числа  $M$  мы уже убедились), то, очевидно, будет достаточно найти все содержащиеся в  $\Omega$  простые делители числа  $M$ . Если мы знаем только, что некоторое (неквадратное) число  $r$  является квадратичным вычетом по модулю  $M$ , то мы уже можем быть уверены, что ни одно простое



число, по которому  $r$  является невычетом, не может быть делителем числа  $M$ ; поэтому из  $\Omega$  можно выбросить все такие простые числа (в большинстве случаев они составляют примерно половину общего количества). Если, кроме того, относительно другого неквадратного числа  $r'$  также известно, что оно является вычетом по модулю  $M$ , то из простых чисел, еще оставшихся в  $\Omega$  после первого исключения, мы снова сможем выкинуть те, по которым  $r'$  является невычетом и которые снова составляют примерно половину общего количества еще оставшихся чисел, если только вычеты  $r$  и  $r'$  независимы один от другого, т. е. если одно из этих чисел не обязательно является вычетом по всем числам, по которым является вычетом второе, что имело бы место в том случае, если бы произведение  $rr'$  было квадратом. Если по модулю  $M$  известны еще и другие вычеты  $r''$ ,  $r'''$ , ..., которые все независимы от остальных, то для каждого из них в отдельности мы можем производить аналогичные исключения, вследствие чего количество чисел в  $\Omega$  будет очень быстро убывать, так что скоро окажутся вычеркнутыми либо все числа из  $\Omega$ , что будет свидетельствовать о том, что  $M$  заведомо есть простое число, либо их останется так мало (при этом, очевидно, останутся все простые делители числа  $M$ , если  $M$  имеет таковые), что делимость на них можно будет уже исследовать без труда. Для числа, не превосходящего миллиона, по большей части оказывается достаточным произвести шесть или семь исключений, для чисел, состоящих из восьми или девяти цифр, — десять или одиннадцать исключений. Мы должны, таким образом, коснуться лишь двух пунктов, во-первых, как находить достаточное количество вычетов по модулю  $M$ , и, во-вторых, как наиболее целесообразным способом производить само исключение. Однако мы начнем со второго вопроса, так как ответ на него покажет нам, какие именно вычеты наиболее удобны для нашей цели.

В четвертом разделе мы подробно показали, как можно отличать те простые числа, по которым некоторое заданное число  $r$  (которое мы можем предполагать не делящимся ни на какой квадрат) явля-

ется вычетом, от тех, по которым оно есть невычет, или, как отличать делители выражения  $x^2 - r$  от неделителей; именно, первые содержатся в некоторых формах вида  $rz + a$ ,  $rz + b, \dots$ , или вида  $4rz + a$ ,  $4rz + b, \dots$ , а вторые — в других аналогичных формах. Если  $r$  достаточно маленькое число, то исключения очень удобно производить при помощи этих формул; например, нужно исключить все числа вида  $4z + 3$ , если  $r = -1$ , все числа вида  $8z + 3$ ,  $8z + 5$ , если  $r = 2$ , и т. д. Но так как находить такие вычеты заданного числа не всегда в наших силах, даже если применение формул для большого значения  $r$  и достаточно удобно, то мы получили бы огромное преимущество и поразительным образом облегчили свой труд при исключении, если бы для достаточно большого количества положительных и отрицательных не делящихся на квадраты чисел  $r$  заранее составили бы *таблицу*, по которой можно было бы отличать простые числа, по которым отдельные  $r$  являются вычетами, от тех, по которым они являются невычетами. Такая таблица может быть устроена таким же образом, как ее образец, приведенный в конце этого сочинения и выше уже описанный; однако для того, чтобы она приносила достаточно большую пользу для нашей настоящей цели, фигурирующие в ней простые числа (модули) должны быть продолжены на много дальше, именно, по меньшей мере до 1000 или 10 000; кроме того, удобство таблицы значительно увеличилось бы, если бы вверху приводились бы также составные и отрицательные числа, хотя, как вытекает из четвертого раздела, это и не является абсолютно необходимым. Удобнее же всего применять такую таблицу, если отдельные вертикальные колонки, из которых она состоит, вырезать и наклеить на полоски жести или (подобно Н е п е р у) на деревянные дощечки, так что те колонки, которые нужны в каждом отдельном случае, т. е. которые соответствуют числам  $r$ ,  $r'$ ,  $r''$ , ..., являющимся вычетами заданного числа, разлагаемого на сомножители, можно рассматривать отдельно. Если приложить их правильным образом к первой колонке таблицы (содержащей модули), т. е. так, что места отдельных дощечек, соответствующих одному и тому же простому числу из первой колонки, лежат на прямом направлении с этим простым числом, или, другими словами, оказываются на одной с ним горизонтальной линии, то те простые числа, которые еще остаются в

$\Omega$  после исключений при помощи вычетов  $r, r', r'', \dots$ , можно будет, очевидно, узнать с одного взгляда; именно, они будут совпадать с теми числами из первой колонки, которым во всех приложенных дощечках соответствуют черточки, а все те, против которых хотя бы в одной дощечке находится пустое место, нужно будет отбросить. Это станет достаточно ясно на примере. Если мы откуда-нибудь знаем, что числа  $-6, +13, -14, +17, +37, -53$  являются вычетами по модулю  $997\,331$ , то нужно приложить к первой колонке (которую в этом случае нужно продолжить до  $997$ , т. е. до наибольшего простого числа, меньшего чем  $\sqrt{997\,331}$ ) полосы, вверху которых стоят числа  $-6, +13, \dots$ . Мы приведем здесь часть получающейся при этом схемы:

|    | $-6$ | $+13$ | $-14$ | $+17$ | $+37$ | $-53$ |
|----|------|-------|-------|-------|-------|-------|
| 3  | —    | —     | —     |       | —     | —     |
| 5  | —    |       | —     |       |       |       |
| 7  | —    |       | —     |       | —     |       |
| 11 | —    |       |       |       | —     |       |
| 13 |      | —     | —     | —     |       | —     |
| 17 |      | —     |       | —     |       | —     |
| 19 |      |       | —     | —     |       | —     |
| 23 |      | —     | —     |       |       | —     |

и т. д.

|     |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|
| 115 |   | — | — |   |   | — |
| 127 | — | — | — | — | — | — |
| 131 | — | — | — |   |   |   |

и т. д.

Подобно тому как мы с одного взгляда узнаем, что из простых чисел, содержащихся в этой части схемы, после исключений при помощи вычетов  $-6, +13, \dots$  в  $\Omega$  остается только число  $127$ , точно так же вся схема, продолженная до числа  $997$ , показывает, что в  $\Omega$  вообще уже не остается никаких других чисел; попробовав же произвести

деление, мы убеждаемся, что 997 331 действительно делится на 127. Таким образом, разложение указанного числа на простые сомножители есть  $127 \cdot 7853$ .

Из изложенного с достаточной ясностью вытекает, что наиболее удобны не очень большие вычеты или, по крайней мере, вычеты, разлагающиеся на не очень большие простые числа, так как непосредственное применение вспомогательной таблицы ограничивается числами, находящимися вверху ее, а вообще таблица применима для чисел, которые могут быть разложены на сомножители, содержащиеся в ней.

### 332

Для нахождения вычетов заданного числа  $M$  мы укажем три различных метода, изложению которых мы предпошлем два замечания, при помощи которых из менее удобных вычетов можно будет получать более простые. *Во-первых*, если число  $ak^2$ , делящееся на квадрат  $k^2$  (который мы предполагаем взаимно простым с  $M$ ), является вычетом по модулю  $M$ , то и число  $a$  будет вычетом; поэтому вычеты, делящиеся на большие квадраты, могут быть сведены к маленьким вычетам, и мы будем предполагать, что все вычеты, находимые при помощи излагаемых далее методов, тотчас же освобождаются от их квадратных сомножителей. *Во-вторых*, если два или несколько чисел являются вычетами, то вычетом будет и их произведение. Если связать это замечание с предыдущим, то очень часто оказывается возможным из нескольких вычетов, которые не все являются достаточно простыми, находить некоторый новый очень простой вычет, если только первые имеют много общих сомножителей. По этой причине очень большую пользу приносят также и такие вычеты, которые составлены из большого количества не слишком больших сомножителей, причем целесообразно сразу же раскладывать эти вычеты на их сомножители. Значение этих замечаний лучше уяснится на примерах и при частом их применении, нежели из теоретических соображений.

I. Простейший, а для тех, кто частым упражнением уже приобрел некоторый опыт, и удобнейший метод состоит в том, что число

$M$ , или, более общо, некоторая его кратность, раскладывается на два слагаемых:  $kM = a + b$  (которые либо оба положительны, либо одно из них положительно, а другое отрицательно); произведение этих слагаемых, взятое с обратным знаком, будет тогда вычетом по модулю  $M$ , так как  $-ab \equiv a^2 \equiv b^2 \pmod{M}$ , и потому  $-abRM$ . Числа  $a, b$  нужно брать такими, чтобы их произведение делилось на большой квадрат, а получающееся при этом частное либо было маленьким, либо по крайней мере раскладывалось на не слишком большие сомножители, чего всегда без труда можно добиться. Особенно рекомендуется брать в качестве  $a$  либо квадрат, либо удвоенный, утроенный и т. д. квадрат, который отличается от  $M$  либо на маленькое число, либо на число, разлагающееся на удобные сомножители. Например, мы находим:  $997\,331 = 999^2 - 2 \cdot 5 \cdot 67 = 994^2 + 5 \cdot 11 \cdot 13^2 = 2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2 = 3 \cdot 575^2 + 11 \cdot 31 \cdot 4^2 = 3 \cdot 577^2 - 7 \cdot 13 \cdot 4^2 = 3 \cdot 578^2 - 7 \cdot 19 \cdot 37 = 11 \cdot 299^2 + 2 \cdot 3 \cdot 5 \cdot 29 \cdot 4^2 = 11 \cdot 301^2 + 5 \cdot 12^2$ , и т. д. Отсюда мы получаем следующие вычеты:  $2 \cdot 5 \cdot 67$ ,  $(-5) \cdot 11$ ,  $(-2) \cdot 3 \cdot 17$ ,  $(-3) \cdot 11 \cdot 31$ ,  $3 \cdot 7 \cdot 13$ ,  $3 \cdot 7 \cdot 19 \cdot 37$ ,  $(-2) \cdot 3 \cdot 5 \cdot 11 \cdot 29$ ; последнее разложение приводит к вычету  $(-5) \cdot 11$ , который мы уже имеем. Вместо вычетов  $-3 \cdot 11 \cdot 31$ ,  $(-2) \cdot 3 \cdot 5 \cdot 11 \cdot 29$  можно взять вычеты  $3 \cdot 5 \cdot 31$ ,  $2 \cdot 3 \cdot 29$ , которые получаются из первых комбинированием их с вычетом  $(-5) \cdot 11$ .

II. Второй и третий методы основаны на том, что если две двойничные формы  $(A, B, C)$ ,  $(A', B', C')$  с одним и тем же определителем  $M$ , или  $-M$ , или вообще,  $\pm kM$ , принадлежат одному и тому же роду, то числа  $AA'$ ,  $AC'$ ,  $A'C$  являются вычетами по модулю  $kM$ ; это без труда устанавливается из того, что каждое характеристическое число  $m$  одной из форм будет характеристическим числом и другой формы, и потому числа  $mA$ ,  $mC$ ,  $mA'$ ,  $mC'$  все будут вычетами по модулю  $kM$ . Поэтому если  $(a, b, a')$  есть приведенная форма с положительным определителем  $M$ , или, более общо,  $kM$ , и если  $(a', b', a'')$ ,  $(a', b'', a''')$ , ... суть формы из ее периода, которые поэтому ей эквивалентны и тем более содержатся с ней в одном роде, то все числа  $aa'$ ,  $aa''$ ,  $aa'''$ , ... будут вычетами по модулю  $M$ . Вычисление большого количества форм такого периода может быть очень легко проведено при помощи алгоритма из п. 187; простейшие вычеты большей частью получаются, если положить  $a = 1$ ; вычеты, содержащие слиш-

ком большие сомножители, следует отбрасывать. Ниже приводятся начала периодов форм  $(1, 998, -1327)$  и  $(1, 1412, -918)$ , определители которых равны  $997\ 331$  и  $1\ 994\ 662$ .

|                     |                      |
|---------------------|----------------------|
| $(1, 998, -1327)$   | $(1, 1412, -918)$    |
| $(-1327, 329, 670)$ | $(-918, 1342, 211)$  |
| $(670, 341, -1315)$ | $(211, 1401, -151)$  |
| $(-1315, 974, 37)$  | $(-151, 1317, 1723)$ |
| $(37, 987, -626)$   | $(1723, 406, -1062)$ |
| $(-626, 891, 325)$  | $(-1062, 656, 1473)$ |
| $(325, 734, -1411)$ | $(1473, 817, -901)$  |
| $(-1411, 677, 382)$ | $(-901, 985, 1137)$  |
| $(382, 851, -715)$  |                      |
| и т. д.             | и т. д.              |

Поэтому все числа  $-1327, 670, \dots$  будут вычетами по модулю  $997\ 331$ . Если из них отбросить те, которые содержат слишком большие сомножители, то останутся следующие:  $2 \cdot 5 \cdot 67, 37, (-17) \cdot 83, (-5) \cdot 11 \cdot 13, (-2) \cdot 3 \cdot 17, (-2) \cdot 59, (-17) \cdot 53$ . Вычет  $2 \cdot 5 \cdot 67$ , так же, как и вычет  $(-5) \cdot 11$ , который получается из комбинации третьего вычета с пятым, мы уже нашли выше.

III. Если  $C$  — некоторый класс, отличный от главного, форм с отрицательным определителем  $-M$  или, более общо,  $-kM$ , и  $2C, 3C, \dots$  — период этого класса (п. 307), то классы  $2C, 4C, \dots$  принадлежат главному роду, а классы  $3C, 5C, \dots$  — тому же роду, что и  $C$ . Если поэтому  $(a, b, c)$  есть (простейшая) форма из  $C$ , и  $(a', b'', c')$  — какая-нибудь форма из некоторого класса указанного периода, например, из  $nC$ , то либо  $a'$ , либо  $aa'$ , в зависимости от того, четно  $n$  или нечетно, будет вычетом по модулю  $M$  (причем в первом случае вычетом, очевидно, будет также и  $c'$ , а во втором —  $ac', ca'$  и  $cc'$ ). Нахождение периода, т. е. форм, простейших в своих классах, производится с поразительной легкостью, когда  $a$  очень мало, особенно в случае  $a = 3$ , чего всегда можно добиться, если сделать предварительно  $kM \equiv 2 \pmod{3}$ . Ниже приводится начало периода класса, в котором содержится форма  $(3, 1, 332444)$ .

|                          |                          |
|--------------------------|--------------------------|
| $C = (3, 1, 332\,444)$   | $6C = (729, -209, 1428)$ |
| $2C = (9, -2, 110\,815)$ | $7C = (476, 209, 2187)$  |
| $3C = (27, 7, 36\,940)$  | $8C = (1027, 342, 1085)$ |
| $4C = (81, 34, 12\,327)$ | $9C = (932, -437, 1275)$ |
| $5C = (243, 34, 4109)$   | $10C = (425, 12, 2347)$  |

Отсюда получаются следующие вычеты (после устранения неудобных):  $3 \cdot 476, 1027, 1085, 425$ , или (если отбросить квадратные сомножители):  $3 \cdot 7 \cdot 17, 13 \cdot 79, 5 \cdot 7 \cdot 31, 17$ , и если их подходящим образом связать с восемью вычетами, найденными в II, мы получим следующие двенадцать вычетов:  $(-2) \cdot 3, 13, (-2) \cdot 7, 17, 37, -53, (-5) \cdot 11, 79, -83, (-2) \cdot 59, (-2) \cdot 5 \cdot 31, 2 \cdot 5 \cdot 67$ . Первые шесть суть те, которыми мы пользовались в п. 331. Можно было бы еще присоединить вычеты  $19$  и  $-29$ , если бы мы хотели использовать также и те, которые были найдены в I; остальные полученные там вычеты уже зависят от найденных здесь.

### 333

**Второй метод разложения заданного числа  $M$  на сомножители** исходит из рассмотрения значений выражения вида  $\sqrt{-D} \pmod{M}$  и основывается на следующих замечаниях.

I. Если  $M$  есть простое число или степень (нечетного, не входящего в  $D$ ) простого числа, то  $-D$  будет вычетом или невычетом по модулю  $M$  в зависимости от того, содержится ли  $M$  в форме делителей или в форме неделителей выражения  $x^2 + D$ , и в первом случае выражение  $\sqrt{-D} \pmod{M}$  обладает только двумя значениями, которые противоположны одно другому.

II. Если же  $M$  есть составное число, и, например, равно  $pr'p''\dots$ , где  $p, p', p'', \dots$  обозначают (нечетные, не входящие в  $D$ , различные) простые числа или степени таких простых чисел, то  $-D$  только тогда будет вычетом по модулю  $M$ , когда  $-D$  есть вычет по всем отдельным числам  $p, p', p'', \dots$ , т. е. когда все эти числа содержатся в формах делителей выражения  $x^2 + D$ . Если же значения выражения  $\sqrt{-D}$  по модулям  $p, p', p'', \dots$  обозначить соответственно через  $\pm r, \pm r',$

$\pm r'', \dots$ , то все значения этого же выражения по модулю  $M$  получатся, если мы найдем числа, которые по модулю  $p$  сравнимы с  $r$  или с  $-r$ , по  $p'$  сравнимы с  $r'$  или  $-r'$  и т. д., так что количество последних значений будет тем самым равно  $2^\mu$ , где  $\mu$  обозначает количество чисел  $p, p', p'', \dots$ . Если теперь эти значения суть  $R, -R, R', -R', R'', \dots$ , то само собой  $R \equiv R$  по всем числам  $p, p', p'', \dots$ ; однако, ни по одному из этих чисел не может иметь места  $R \equiv -R$ , так что наибольший общий делитель чисел  $M$  и  $R - R$  равен  $M$ , а наибольший общий делитель чисел  $M$  и  $R + R$  равен 1; всякие же два значения, которые не являются ни совпадающими, ни противоположными, как, например,  $R$  и  $R'$ , будут обязательно сравнимы по одному или нескольким (но не по всем) из чисел  $p, p', p'', \dots$ , по остальным же будет иметь место  $R \equiv -R'$ ; поэтому произведение первых есть наибольший общий делитель чисел  $M$  и  $R - R'$ , а произведение последних — наибольший общий делитель чисел  $M$  и  $R + R'$ . Отсюда легко видеть, что если вычислены все наибольшие общие делители числа  $M$  с разностями между отдельными значениями выражения  $\sqrt{-D} \pmod{M}$  и каким-нибудь данным значением, то эта совокупность будет содержать числа  $1, p, p', p'', \dots$ , а также их произведения по два, по три и т. д. Таким образом, мы оказываемся в состоянии по значениям указанного выражения определить числа  $p, p', p'', \dots$ .

Впрочем, так как метод п. 327 сводит эти отдельные значения к значениям выражений вида  $\frac{m}{n} \pmod{M}$ , где знаменатель  $n$  взаимно прост с  $M$ , то сами значения нам и не нужно находить. Действительно, наибольший общий делитель числа  $M$  и разности между  $R$  и  $R'$ , которые совпадают с  $m/n$  и  $m'/n'$ , является, очевидно, также и наибольшим общим делителем числа  $M$  и  $nn'(R - R')$ , а, значит, также чисел  $M$  и  $mn' - nm'$ , так как последнее число сравнимо с  $nn'(R - R')$  по модулю  $M$ .

Предыдущие замечания могут быть использованы в настоящем вопросе двояким образом; используя первый способ, мы не только сможем узнать, является ли заданное число  $M$  простым или составным, но и сможем в последнем случае найти сомножители; второй способ заслуживает предпочтения в том отношении, что он в большин-



стве случаев требует более простых вычислений, однако, если не применять его многократно, он не всегда дает самые сомножители составных чисел, хотя при помощи него также можно отличать составные числа от простых.

I. Найдем отрицательное число  $-D$ , которое является квадратичным вычетом по модулю  $M$ ; для этой цели можно использовать методы, указанные в п. 332, I и II. Хотя, вообще говоря, и безразлично, какой вычет мы выберем, причем, в отличие от предыдущего метода, здесь вовсе нет нужды, чтобы  $D$  было маленьким числом, тем не менее вычисления будут тем короче, чем меньше число классов двойничных форм, содержащихся в отдельных собственно примитивных родах с определителем  $-D$ , так что особенно благоприятны те вычеты, если только они годятся, которые содержатся среди 65 чисел п. 303. Так, для  $M = 997\ 331$  среди всех найденных выше отрицательных вычетов наиболее удобным является вычет  $-102$ . Далее найдем все различные значения выражения  $\sqrt{-D} \pmod{M}$ ; если их окажется только два (противоположных), то  $M$  заведомо является простым числом или степенью простого числа; если же их будет больше, а именно,  $2^\mu$ , то  $M$  будет состоять из  $\mu$  различных простых чисел или степеней простых чисел, и эти сомножители могут быть найдены методом предыдущего пункта. Являются ли эти сомножители простыми числами или степенями простых чисел, можно не только легко определить непосредственно, но и сам метод, при помощи которого отыскиваются значения выражения  $\sqrt{-D}$ , непосредственно указывает те простые числа, которые входят в  $M$  в некоторых степенях, больших 1. Именно, если  $M$  делится на квадрат простого числа  $\pi$ , то при указанных вычислениях мы заведомо придем хотя бы к одному такому представлению  $M = at^2 + 2btp + cn^2$  числа  $M$ , для которого наибольший общий делитель чисел  $t, p$  равен  $\pi$  (вследствие того, что в этом случае  $-D$  будет также вычетом и по модулю  $M/\pi^2$ ). Если же не получится ни одного представления, у которого  $t$  и  $p$  имеют общий делитель, то это будет верным признаком, что  $M$  не делится ни на какой квадрат, и потому все числа  $p, p', p'', \dots$  являются простыми.

Пример. Указанным выше методом мы находим четыре значения выражения  $\sqrt{-408} \pmod{997\ 331}$ , которые совпадают со зна-

чениями  $\pm \frac{1664}{113}$ ,  $\pm \frac{2824}{3}$ ; в качестве наибольших общих делителей числа 997 331 и чисел  $3 \cdot 1164 - 113 \cdot 2824 = 314\ 120$  и  $3 \cdot 1164 + 113 \cdot 2824 = 324\ 104$  мы находим соответственно 7853 и 127, поэтому  $997\ 331 = 127 \cdot 7853$ , как и выше.

II. Возьмем какое-нибудь отрицательное число  $-D$  с тем свойством, что  $M$  содержится в форме делителей выражения  $x^2 + D$ . Само по себе безразлично, какое именно число такого рода взять; однако ради удобства нужно в первую очередь обратить внимание на то, чтобы количество классов в родах с определителем  $-D$  было по возможности маленьким. Кстати, получение такого числа не сталкивается ни с какими трудностями, если мы ищем его посредством проб; действительно, в большинстве случаев при достаточном количестве испробованных чисел число  $M$  оказывается примерно столько же раз в форме делителей, что и в форме неделителей. Поэтому целесообразнее всего начинать пробы с 65 чисел п. 303 (и притом с наибольших из них) и только если окажется, что ни одно из них не годится (что, однако, вообще говоря случается один раз из 16 384), переходить к другим числам, для которых в отдельных родах содержится по два класса. Затем мы получаем значения выражения  $\sqrt{-D} \pmod{M}$  и выводим из них, точно таким же образом, как и выше, сомножители числа  $M$ . Если же таких значений не получится, т. е.  $-D$  окажется квадратичным невычетом по модулю  $M$ , то, значит,  $M$  заведомо не может быть ни простым числом, ни степенью простого числа. Если в последнем случае мы хотим найти сами сомножители, то нужно либо повторить ту же операцию, взяв в качестве  $D$  другое значение, либо прибегнуть к другим методам.

Если мы, например, произведем исследование числа 997 331, то найдем, что оно содержится в форме неделителей выражений  $x^2 + 1848$ ,  $x^2 + 1365$ ,  $x^2 + 1320$ , но в форме делителей выражения  $x^2 + 840$ ; в качестве значений выражения  $\sqrt{-840} \pmod{997\ 331}$  мы получаем выражения  $\pm \frac{1272}{163}$ ,  $\pm \frac{3288}{125}$ , откуда получаются те же сомножители, что и выше. Желаящие иметь другие примеры могут обратиться к п. 328, где первый пример показывает, что  $5\ 428\ 681 = 307 \cdot 17\ 683$ , второй, — что  $4\ 272\ 943$  является про-

стым числом, и третий,— что число 997 331 заведомо составлено из нескольких простых чисел.

Впрочем, границы настоящего сочинения позволили изложить лишь основные моменты обоих методов нахождения сомножителей; более подробное исследование с привлечением большего количества вспомогательных таблиц и других вспомогательных средств мы откладываем до другого случая.

---

---

## РАЗДЕЛ VII

### ОБ УРАВНЕНИЯХ, ОТ КОТОРЫХ ЗАВИСИТ ДЕЛЕНИЕ КРУГА

335

Среди наиболее блестящих достижений, которыми обогатилась математика благодаря работам ученых последнего времени, особенно выдающееся место, без сомнения, занимает теория функций, связанных с кругом. На этот замечательный тип величин, к которому приходишь при самых различных исследованиях и без помощи которого не может обойтись ни одна часть всей математики, крупнейшие из новых математиков столь усердно направляли свое прилежание и остроумие, и создали столь обширную теорию, что почти невозможно было ожидать, чтобы еще какая-нибудь часть этой теории, тем более часть, находящаяся у самых истоков и вполне элементарная, допускала бы еще более важное развитие. Я имею в виду теорию тригонометрических функций, соответствующих дугам, которые соизмеримы с длиной окружности, или теорию правильных многоугольников; настоящий раздел покажет, насколько незначительная часть ее была разработана до сих пор. Читатель может удивиться, что это исследование помещено именно в настоящем труде, который, на первый взгляд, посвящен совершенно чуждому этим вопросам предмету; однако само сочинение достаточно убедительно покажет, в какой тесной связи с высшей арифметикой эти вопросы находятся.

Впрочем, принципы теории, к изложению которой мы теперь переходим, распространяются намного дальше того, чем они развиты

здесь. Действительно, они могут быть применены не только к круговым функциям, но и ко многим другим трансцендентным функциям, например, к тем, которые зависят от интеграла  $\int \frac{dx}{\sqrt{1-x^4}}$ , и, кроме того, к различным типам сравнений; но так как об указанных трансцендентных функциях мы готовим специальное обширное сочинение, а о сравнениях подробно будет идти речь в продолжении арифметических исследований, нам показалось целесообразным рассматривать здесь только круговые функции. И даже эти функции, которые мы могли бы рассматривать во всей общности, мы при помощи излагаемых в следующем пункте приемов сведем к простейшему случаю, — с одной стороны, ради краткости, а с другой — потому, что благодаря этому станут более понятными совершенно новые принципы этой теории.

**Исследование сводится к простейшему случаю,  
когда число частей, на которые должен быть разбит круг,  
является простым**

### 336

Если обозначить окружность или четыре прямых угла через  $P$  и предположить, что  $m$  и  $n$  — целые числа, причем  $n$  есть произведение попарно взаимно простых сомножителей  $a, b, c, \dots$ , то, согласно п. 310, угол  $A = \frac{mP}{n}$  может быть представлен в виде

$A = \left( \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \dots \right) P$ , и соответствующие ему тригонометрические функции могут быть известными методами получены из функций, соответствующих частям  $\alpha P/a, \beta P/b, \dots$ . Но так как в качестве  $a, b, c, \dots$  можно взять простые числа или степени простых чисел, то достаточно, очевидно, рассматривать только деление круга на части, число которых является простым или равно степени простого числа, а многоугольник с  $n$  сторонами тотчас же можно получить из многоугольников с  $a, b, c, \dots$  сторонами. Мы, однако, ограничимся здесь в нашем исследовании тем случаем, когда круг нужно делить на части, число которых является (нечетным) простым, и делаем мы это в

первую очередь по следующей причине. Как известно, круговые функции, соответствующие углу  $\frac{mP}{p^2}$ , могут быть получены посредством решения уравнения  $p$ -й степени из функций, соответствующих углу  $\frac{mP}{p}$ , а из первых посредством решения уравнения такой же степени могут быть получены функции, соответствующие углу  $\frac{mP}{p^3}$  и т. д., так что если мы уже имеем многоугольник с  $p$  сторонами, то для определения многоугольника с  $p^\lambda$  сторонами нужно решить  $\lambda - 1$  уравнений  $p$ -й степени. И хотя дальнейшая теория могла бы быть применена также и к этому случаю, но и на этом пути мы пришли бы к такому же числу уравнений  $p$ -й степени, которая, когда  $p$  простое число, никак не может быть понижена. Например, ниже будет показано, что многоугольник с 17 сторонами может быть построен геометрически; однако для определения многоугольника с 289 сторонами никак нельзя избежать уравнения 17-й степени.

**Уравнения для тригонометрических функций дуг,  
составляющих одну или несколько частей полной окружности;  
сведение тригонометрических функций к корням уравнения**  
 $x^n - 1 = 0$

337

Хорошо известно, что тригонометрические функции всех углов вида  $\frac{kP}{n}$ , где  $k$  пробегает числа  $0, 1, 2, \dots, n - 1$ , выражается через корни уравнений  $n$ -й степени, причем *синус* выражается через корни уравнения

$$\text{I. } x^n - \frac{1}{4} nx^{n-2} + \frac{1}{16} \frac{n(n-3)}{1 \cdot 2} x^{n-4} - \\ - \frac{1}{64} \frac{n(n-4)(n-5)}{1 \cdot 2 \cdot 3} x^{n-6} + \dots \pm \frac{1}{2^{n-1}} nx = 0,$$

*косинус* — через корни уравнения

$$\text{II. } x^n - \frac{1}{4} nx^{n-2} + \frac{1}{16} \frac{n(n-3)}{1 \cdot 2} x^{n-4} - \\ - \frac{1}{64} \frac{n(n-4)(n-5)}{1 \cdot 2 \cdot 3} x^{n-6} + \dots \pm \frac{1}{2^{n-1}} nx - \frac{1}{2^{n-1}} = 0,$$

и наконец, *тангенс* — через корни уравнения

$$\text{III. } x^n - \frac{n(n-1)}{1 \cdot 2} x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} x^{n-4} - \dots \pm nx = 0.$$

Эти уравнения, которые, вообще говоря, имеют место для каждого нечетного значения  $n$  (уравнение II также и для четного), могут быть сведены, если положить  $n = 2m + 1$ , к  $m$ -й степени; именно, уравнения I и III нужно разделить на  $x$  и положить  $y = x^2$ . Уравнение II, очевидно, имеет корень  $x = 1$  ( $= \cos 0$ ), а остальные его корни разбиваются на попарно равные  $\left( \cos \frac{P}{n} = \cos \frac{(n-1)P}{n}, \cos \frac{2P}{n} = \cos \frac{(n-2)P}{n}, \dots \right)$ ; поэтому левая часть делится на  $x - 1$ , и частное является квадратом; если из него извлечь квадратный корень, то уравнение II приведет к уравнению

$$x^m + \frac{1}{2} x^{m-1} - \frac{1}{4} (m-1) x^{m-2} - \frac{1}{8} (m-2) x^{m-3} + \\ + \frac{1}{16} \frac{(m-2)(m-3)}{1 \cdot 2} x^{m-4} + \frac{1}{32} \frac{(m-3)(m-4)}{1 \cdot 2} x^{m-5} - \dots = 0,$$

корнями которого являются косинусы углов  $P/n, 2P/n, 3P/n, \dots, mP/n$ . Дальнейших редукций для этих уравнений, по крайней мере в случае, когда  $n$  есть простое число, до сих пор не было известно.

Между тем ни одно уравнение не является столь простым для рассмотрения и удобным для нашей цели, как уравнение  $x^n - 1 = 0$ , корни которого, как известно, теснейшим образом связаны с корнями указанных уравнений. Именно, если обозначить для краткости мнимую величину  $\sqrt{-1}$  через  $i$ , то корни уравнения  $x^n - 1 = 0$  представятся в виде

$$\cos \frac{kP}{n} + i \sin \frac{kP}{n} = r,$$

где в качестве  $k$  нужно брать все числа  $0, 1, 2, 3, \dots, n-1$ . Но

так как  $\frac{1}{r} = \cos \frac{kP}{n} - i \sin \frac{kP}{n}$ , то корни уравнения I представятся в виде  $(r - \frac{1}{r})/2i$  или  $i(1 - r^2)/2r$ , корни уравнения II — в виде  $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+r^2}{2r}$ , наконец, корни уравнения III — в виде  $i(1 - r^2)/(1 + r^2)$ . По этой причине мы будем основывать наше исследование на рассмотрении уравнения  $x^n - 1 = 0$ , причем будем предполагать, что  $n$  является нечетным простым числом. А для того чтобы дальше не пришлось прерывать последовательность рассуждений, мы предположим здесь следующее вспомогательное предложение.

338

**Задача.** Пусть задано уравнение

$$(W) \quad z^m + Az^{m-1} + \dots = 0;$$

нужно найти уравнение  $(W')$ , корни которого являются  $\lambda$ -ми степенями корней уравнения  $(W)$ , где  $\lambda$  обозначает заданный положительный целый показатель степени.

**Решение.** Если обозначить корни уравнения  $(W)$  через  $a, b, c, \dots$ , то корнями уравнения  $(W')$  должны быть  $a^\lambda, b^\lambda, c^\lambda, \dots$ . Согласно известной теореме Ньютона, по коэффициентам уравнения  $(W)$  можно найти суммы любых степеней корней  $a, b, c, \dots$ . Итак, найдем суммы

$$a^\lambda + b^\lambda + c^\lambda + \dots; \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} + \dots, \quad \dots \text{ до } a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \dots$$

В свою очередь по этим суммам можно будет затем определить при помощи той же теоремы коэффициенты уравнения  $(W')$ . Одновременно из этого вытекает, что если коэффициенты у  $(W)$  рациональны, то и все коэффициенты у  $(W')$  тоже будут рациональными. Другим путем можно даже доказать, что если первые являются целыми числами, то и вторые будут целыми числами; однако мы не будем здесь останавливаться на этой теореме, которая не столь уж нужна для нашей цели.



## Теория корней уравнения $x^n - 1 = 0$

(в предположении, что  $n$  есть простое число).

Если отбросить корень 1, то совокупность  $(\Omega)$  остальных корней содержится в уравнении  $X = x^{n-1} + x^{n-2} + \dots + x + 1 = 0$

339

Уравнение  $x^n - 1 = 0$  (где все время подразумевается, что  $n$  есть простое число) имеет только один вещественный корень  $x = 1$ ; остальные  $n - 1$  корней, которые охватываются уравнением

$$x^{n-1} + x^{n-2} + \dots + x + 1 = 0,$$

все являются мнимыми; совокупность их мы обозначим через  $\Omega$ , а функцию

$$x^{n-1} + x^{n-2} + \dots + x + 1$$

через  $X$ . Таким образом, если  $r$  есть какой-нибудь корень из  $\Omega$ , то  $1 = r^n = r^{2n}$ , и т. д., и вообще  $r^{en} = 1$  для каждого положительного или отрицательного значения  $e$ ; отсюда очевидно, что если  $\lambda, \mu$  суть сравнимые по модулю  $n$  целые числа, то  $r^\lambda = r^\mu$ . Если же  $\lambda, \mu$ , напротив, не сравнимы по модулю  $n$ , то  $r^\lambda$  и  $r^\mu$  будут не равны; действительно, в этом случае можно найти такое целое число  $\nu$ , что  $(\lambda - \mu)\nu \equiv 1 \pmod{n}$ , откуда следует, что  $r^{(\lambda - \mu)\nu} = r$  и потому  $r^{\lambda - \mu}$  заведомо не равно 1. Далее, ясно, что каждая степень корня  $r$  также является корнем уравнения  $x^n - 1 = 0$ ; поэтому, так как все величины  $1 (= r^0), r, r^2, \dots, r^{n-1}$  различны, они будут представлять собой все корни уравнения  $x^n - 1 = 0$ , и потому совокупность  $r, r^2, r^3, \dots, r^{n-1}$  будет совпадать с  $\Omega$ . Отсюда мы легко заключаем, что, вообще,  $\Omega$  совпадает с любой совокупностью  $r^e, r^{2e}, r^{3e}, \dots, r^{(n-1)e}$ , где  $e$  обозначает некоторое целое не делящееся на  $n$  положительное или отрицательное число. Поэтому

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \dots (x - r^{(n-1)e}),$$

откуда следует:

$$r^e + r^{2e} + r^{3e} + \dots + r^{(n-1)e} = -1 \quad \text{и} \quad 1 + r^e + r^{2e} + r^{3e} + \dots + r^{(n-1)e} = 0.$$

Два таких корня, как  $r$  и  $\frac{1}{r}$  ( $= r^{n-1}$ ) или, вообще,  $r^e$  и  $r^{-e}$ , мы будем называть обратными; очевидно, что произведение двух простых сомножителей  $x - r$  и  $x - \frac{1}{r}$  вещественно, именно, равно  $x^2 - 2x \cos \omega + 1$ , так что угол  $\omega$  равен либо углу  $P/n$ , либо некоторой его кратности.

## 340

Так как тем самым, если один из корней из  $\Omega$  обозначен через  $r$ , то все корни уравнения  $x^n - 1 = 0$  представляются в виде степеней  $r^\lambda$ , то, следовательно, произведение нескольких корней этого уравнения также может быть представлено в виде  $r^\lambda$ , где  $\lambda$  либо равно 0, либо положительно и меньше, чем  $n$ . Поэтому, если обозначить через  $\varphi(t, u, v, \dots)$  алгебраическую целую рациональную функцию от неизвестных  $t, u, v, \dots$ , которую можно представить в виде суммы слагаемых вида  $ht^\alpha u^\beta v^\gamma \dots$ , то ясно, что если вместо  $t, u, v, \dots$  подставить некоторые корни уравнения  $x^n - 1 = 0$ , скажем, положить  $t = a, u = b, v = c, \dots$ , то функцию  $\varphi(a, b, c, \dots)$  можно будет представить в виде

$$A + A'r + A''r^2 + A'''r^3 + \dots + A^{(n-1)}r^{n-1},$$

где коэффициенты  $A, A', \dots$  (из которых некоторые могут отсутствовать, т. е. быть равны 0) будут определенными величинами, и, кроме того, все эти коэффициенты будут целыми числами, если все постоянные коэффициенты у  $\varphi(t, u, v, \dots)$ , т. е. все числа  $h$  будут целыми. Если же затем вместо  $t, u, v, \dots$  подставить соответственно  $a^2, b^2, c^2, \dots$ , то каждое слагаемое вида  $ht^\alpha u^\beta v^\gamma \dots$ , которое перед этим давало  $r^\sigma$ , теперь даст  $r^{2\sigma}$ , откуда легко видеть, что

$$\varphi(a^2, b^2, c^2, \dots) = A + A'r^2 + A''r^4 + A'''r^6 + \dots + A^{(n-1)}r^{2n-2}.$$

Точно так же и вообще для любого целого значения  $\lambda$

$$\varphi(a^\lambda, b^\lambda, c^\lambda, \dots) = A + A'r^\lambda + A''r^{2\lambda} + \dots + A^{(n-1)}r^{(n-1)\lambda};$$

эта теорема имеет очень большое значение и составляет основу дальнейших исследований.

Отсюда следует, далее, что

$$\varphi(1, 1, 1, \dots) = \varphi(a^n, b^n, c^n, \dots) = A + A' + A'' + \dots + A^{(n-1)},$$

и

$$\begin{aligned} \varphi(a, b, c, \dots) + \varphi(a^2, b^2, c^2, \dots) + \varphi(a^3, b^3, c^3, \dots) + \dots \\ \dots + \varphi(a^n, b^n, c^n, \dots) = nA, \end{aligned}$$

так что эта сумма всегда является целым числом, делящимся на  $n$ , если все постоянные коэффициенты у  $\varphi(t, u, v, \dots)$  целые.

**Функция  $X$  не может быть разложена на сомножители более низких степеней, все коэффициенты у которых рациональны**

### 341

**Теорема.** Если функция  $X$  делится на функцию

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \dots + Kx + L$$

более низкой степени, то коэффициенты  $A, B, \dots, L$  не могут быть все одновременно целыми числами.

**Доказательство.** Пусть  $X = PQ$  и  $\mathfrak{P}$  есть совокупность корней уравнения  $P = 0$ , а  $\mathfrak{Q}$  — совокупность корней уравнения  $Q = 0$ , так что  $\Omega$  состоит из  $\mathfrak{P}$  и  $\mathfrak{Q}$ . Далее, пусть  $\mathfrak{R}$  есть совокупность корней, обратных корням из  $\mathfrak{P}$ , и  $\mathfrak{S}$  — совокупность корней, обратных корням из  $\mathfrak{Q}$ , и пусть корни, которые содержатся в  $\mathfrak{R}$ , являются корнями уравнения  $R = 0$  (которое, как легко видеть, есть  $x^\lambda + \frac{K}{L}x^{\lambda-1} + \dots + \frac{A}{L}x + \frac{1}{L} = 0$ ), а корни, которые содержатся в  $\mathfrak{S}$ , являются корнями уравнения  $S = 0$ . Очевидно, что корни из  $\mathfrak{R}$  и  $\mathfrak{S}$  вместе также будут составлять всю совокупность  $\Omega$  и что  $RS = X$ . Теперь мы будем различать четыре случая.

I.  $\mathfrak{P}$  совпадает с  $\mathfrak{R}$  и потому  $P = R$ . В этом случае, очевидно, корни из  $\mathfrak{P}$  будут попарно обратны, и потому  $P$  будет произведением  $\lambda/2$  удвоенных сомножителей вида  $x^2 - 2x \cos \omega + 1$ ; так как каждый такой сомножитель равен  $(x - \cos \omega)^2 + \sin^2 \omega$ , то легко видеть, что  $P$  при любом вещественном значении  $x$  обяза-

тельно принимает вещественное положительное значение. Пусть уравнения, корнями которых являются квадраты, кубы, биквадраты, и т. д., наконец,  $(n-1)$ -е степени корней из  $\mathfrak{F}$ , суть  $P'=0$ ,  $P''=0$ ,  $P'''=0, \dots, P^{(n-1)}=0$ , и пусть значения функций  $P, P', P'', \dots, P^{(n-1)}$ , которые они принимают при  $x=1$ , равны соответственно  $p, p', p'', \dots, p^{(n-1)}$ ; тогда, согласно сказанному перед этим,  $p$  будет величиной положительной, и по совершенно аналогичной причине  $p', p'', \dots$  также будут положительными. Но так как  $p$  есть значение функции  $(1-t)(1-u)(1-v)\dots$ , которое она принимает, если в качестве  $t, u, v, \dots$  подставить корни из  $\mathfrak{F}$ ,  $p'$  — значение этой же функции, которое она принимает, если вместо  $t, u, v, \dots$  подставить квадраты этих корней, и т. д.; так как, кроме того, значение функции при  $t=1, u=1, v=1$ , очевидно, равно 0, то сумма  $p + p' + p'' + \dots + p^{(n-1)}$  является целым не делящимся на  $n$  числом. Кроме того, легко видеть, что  $P \cdot P' \cdot P'' \dots = X^\lambda$ , и потому  $p \cdot p' \cdot p'' \dots = n^\lambda$ .

Если бы теперь все коэффициенты у  $P$  были рациональны, то, согласно п. 338, были бы рациональны также и все коэффициенты у  $P', P'', \dots$ ; согласно же п. 42, все эти коэффициенты обязательно были бы целыми числами. Поэтому и  $p, p', p'', \dots$  были бы целыми числами, а так как их произведение равно  $n^\lambda$ , а их количество  $n-1 > \lambda$ , то обязательно некоторые из них (по меньшей мере  $n-1-\lambda$ ) были бы равны 1, а остальные были бы равны либо  $n$ , либо некоторой степени числа  $n$ . Но если бы  $g$  из них были бы равны 1, то, очевидно, имело бы место  $p + p' + \dots \equiv g \pmod{n}$ , и потому эта сумма заведомо не делилась бы на  $n$ . Поэтому сделанное предположение неверно.

II. Если  $\mathfrak{F}$  и  $\mathfrak{K}$  хотя и не совпадают, но все же имеют несколько общих корней, то пусть  $\mathfrak{X}$  их совокупность, и  $T=0$  — уравнение, корнями которого они являются. Тогда  $T$  будет наибольшим общим делителем функций  $P, R$  (что известно из теории уравнений). Но очевидно, что в  $\mathfrak{X}$  корни будут попарно обратными, и потому, согласно только что доказанному, не может быть, чтобы все коэффициенты у  $T$  были рациональными. Однако они все были бы рациональными (что вытекает из природы операций, посредством которых находится наибольший общий делитель), если бы

были рациональными все коэффициенты у  $P$ , а, следовательно, и все коэффициенты у  $R$ . Поэтому наше предположение приводит к противоречию.

III. Если  $\mathfrak{Q}$  и  $\mathfrak{S}$  либо совпадают, либо по крайней мере имеют общие корни, то по совершенно аналогичной причине не может быть, чтобы все коэффициенты у  $Q$  были рациональны; однако они оказались бы рациональными, если бы были рациональны все коэффициенты у  $P$ . Поэтому последнее невозможно.

IV. Наконец, если бы ни  $\mathfrak{P}$  с  $\mathfrak{K}$ , ни  $\mathfrak{Q}$  с  $\mathfrak{S}$  не имели общих корней, то все корни из  $\mathfrak{P}$  содержались бы в  $\mathfrak{S}$ , и все корни из  $\mathfrak{Q}$  — в  $\mathfrak{K}$ , так что было бы  $P = S$  и  $Q = R$ . Поэтому  $X = PQ$  было бы произведением  $P$  и  $R$ , т. е. произведением

$$x^\lambda + Ax^{\lambda-1} + \dots + Kx + L \text{ на } x^\lambda + \frac{K}{L}x^{\lambda-1} + \dots + \frac{A}{L}x + \frac{1}{L},$$

откуда, полагая  $x = 1$ , мы получили бы

$$nL = (1 + A + \dots + K + L)^2.$$

Но если бы все коэффициенты у  $P$  были рациональными, а потому, согласно п. 42, также и целыми, то  $L$ , которое должно было бы входить в последний коэффициент функции  $X$ , т. е. в 1, обязательно было бы равно  $\pm 1$ , вследствие чего  $n$  было бы точным квадратом. Поскольку это противоречит предположению, наше допущение не верно.

Таким образом, из этой теоремы вытекает, что если бы  $X$  можно было разложить на сомножители, то по крайней мере часть их коэффициентов была бы иррациональна, т. е. определялась бы уравнениями более высоких степеней.

**Указывается цель дальнейших исследований**

*Цель дальнейших исследований, указать которую представляется небесполезным, состоит в том, чтобы последовательно разлагать  $X$  на все большее и большее число сомножителей, причем так, чтобы их коэффициенты определялись при помощи уравнений по возмож-*

ности более низких степеней, пока мы не дойдем таким путем до простых сомножителей, т. е. до самих корней из  $\Omega$ . Именно, мы покажем, что если число  $n - 1$  каким-либо способом разложено на целочисленные сомножители  $\alpha, \beta, \gamma, \dots$  (которые можно считать простыми числами), то  $X$  можно разложить на  $\alpha$  сомножителей степени  $(n - 1) / \alpha$ , коэффициенты которых определяются уравнением степени  $\alpha$ ; далее, что эти отдельные сомножители в свою очередь могут быть разложены на  $\beta$  сомножителей степени  $(n - 1) / \alpha\beta$  при помощи уравнения степени  $\beta$  и т. д., так что если  $\nu$  обозначает число сомножителей  $\alpha, \beta, \gamma, \dots$ , то нахождение корней из  $\Omega$  сводится к решению  $\nu$  уравнений степеней  $\alpha, \beta, \gamma$  и т. д. Так, например, для  $n = 17$ , где  $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ , придется решить четыре квадратных, а для  $n = 73$  — три квадратных и два кубических уравнения.

Так как в дальнейшем очень часто придется рассматривать такие степени корня  $r$ , показатели которых в свою очередь являются степенями, а писать такие выражения довольно громоздко, мы в дальнейшем для облегчения изложения будем использовать следующее сокращенное обозначение: вместо  $r, r^2, r^3, \dots$  мы будем писать  $[1], [2], [3], \dots$  и вообще, вместо  $r^\lambda$ , где  $\lambda$  обозначает любое целое число, будем писать  $[\lambda]$ . Таким образом, подобные выражения становятся вполне определенными только после того, как в качестве  $r$ , т. е.  $[1]$ , взят определенный корень из  $\Omega$ . Вообще же  $[\lambda], [\mu]$  будут равны или не равны в зависимости от того, сравнимы или не сравнимы  $\lambda, \mu$  по модулю  $n$ ; далее, имеет место  $[0] = 1$ ;  $[\lambda] \cdot [\mu] = [\lambda + \mu]$ ;  $[\lambda]^\nu = [\lambda\nu]$ ; сумма  $[0] + [\lambda] + [2\lambda] + \dots + [(n - 1)\lambda]$  равна либо 0, либо  $n$ , в зависимости от того, не делится  $\lambda$  на  $n$  или делится.

**Все корни из  $\Omega$   
разбиваются на некоторые классы (периоды)**

Если число  $g$  является для модуля  $n$  числом такого рода, которые мы в разделе III называли первообразными корнями, то  $n - 1$  чисел  $1, g, g^2, \dots, g^{n-2}$  будут сравнимы по модулю  $n$ , быть

может, только в другом порядке, с числами  $1, 2, 3, \dots, n-1$ , т. е. каждое число одного ряда имеет сравнимое с ним число во втором ряду. Отсюда непосредственно следует, что совокупность корней  $[1], [g], [g^2], \dots, [g^{n-2}]$  совпадает с  $\Omega$ , и точно так же вообще с  $\Omega$  будет совпадать любая совокупность

$$[\lambda], [\lambda g], [\lambda g^2], \dots, [\lambda g^{n-2}],$$

где  $\lambda$  обозначает любое целое число, не делящееся на  $n$ . Далее, легко видеть, в силу того, что  $g^{n-1} \equiv 1 \pmod{n}$ , что корни  $[\lambda g^\mu], [\lambda g^\nu]$  будут совпадающими или различными в зависимости от того, сравнимы  $\mu, \nu$  по модулю  $n$  или не сравнимы.

Если теперь  $G$  есть другой первообразный корень, то корни  $[1], [g], \dots, [g^{n-2}]$  будут, с точностью до порядка расположения, совпадать также с  $[1], [G], \dots, [G^{n-2}]$ . Но, кроме того, легко доказывается, что если  $e$  есть делитель числа  $n-1$ , и  $n-1 = ef$ ,  $g^e = h$ ,  $G^e = H$ , то также и  $f$  чисел  $1, h, h^2, \dots, h^{f-1}$  будут (с точностью до порядка расположения) сравнимы с числами  $1, H, H^2, \dots, H^{f-1}$ . Действительно, если мы предположим, что  $G \equiv g^\omega \pmod{n}$ , и  $\mu$  есть произвольное положительное число, которое меньше чем  $f$ , а  $\nu$  — наименьший вычет числа  $\mu\omega$  по модулю  $f$ , то будет иметь место  $\nu e \equiv \mu\omega e \pmod{n-1}$ , откуда  $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$  или  $H^\nu \equiv h^\mu$ , т. е. для каждого числа второго ряда  $1, H, H^2, \dots$  в первом ряду имеется сравнимое с ним, и наоборот. Из этого вытекает, что совокупность  $f$  корней  $[1], [h], [h^2], \dots, [h^{f-1}]$  совпадает с совокупностью корней  $[1], [H], [H^2], \dots, [H^{f-1}]$ , и, более общо, что  $[\lambda], [\lambda h], [\lambda h^2], \dots, [\lambda h^{f-1}]$  совпадает с  $[\lambda], [\lambda H], [\lambda H^2], \dots, [\lambda H^{f-1}]$ . Сумму  $f$  корней вида  $[\lambda] + [\lambda h] + [\lambda h^2] + \dots + [\lambda h^{f-1}]$ , которую нужно рассматривать как не зависящую от  $g$ , так как она не меняется, если вместо  $g$  взять другой первообразный корень, мы будем обозначать через  $(f, \lambda)$ , а совокупность этих корней будем называть периодом  $(f, \lambda)$ , причем порядок расположения корней не принимается во внимание \*. При представлении такого периода будет целесообразно заменять отдельные корни, из которых он состоит, их простей-

\* Может случиться, что мы, когда из-за этого не смогут возникнуть недоразумения, будем в дальнейшем называть саму сумму численным значением периода или просто периодом.

шими выражениями, а именно, вместо чисел  $\lambda, \lambda h, \lambda h^2, \dots$  подставлять их наименьшие вычеты по модулю  $n$ , по величине которых можно при желании также и упорядочивать слагаемые периода.

**Пример.** Для  $n = 19$ , когда в качестве первообразного корня взято число 2, период  $(6, 1)$  состоит из корней  $[1], [8], [64], [512], [4096], [32\,768]$  или из корней  $[1], [7], [8], [11], [12], [18]$ . Точно так же период  $(6, 2)$  состоит из корней  $[2], [3], [5], [14], [16], [17]$ . Период  $(6, 3)$  совпадает с предыдущим. Период  $(6, 4)$  содержит корни  $[4], [6], [9], [10], [13], [15]$ .

## Различные теоремы о периодах корней из $\Omega$

344

Относительно этих периодов сразу же можно сделать следующие замечания.

I. Так как  $\lambda h^f \equiv \lambda, \lambda h^{f+1} \equiv \lambda h, \dots \pmod{n}$ , то очевидно, что  $(f, \lambda h), (f, \lambda h^2), \dots$  будут состоять из тех же корней, что и  $(f, \lambda)$ ; таким образом, если  $[\lambda']$  обозначает любой корень из периода  $(f, \lambda)$  то этот период будет полностью совпадать с периодом  $(f, \lambda')$ . Если поэтому два периода, содержащие одинаковое число корней (такие периоды мы будем называть **однотипными**) имеют хотя бы один общий корень, то они, очевидно, будут совпадать. Следовательно, не может быть, чтобы в одном из двух однотипных периодов содержались какие-нибудь два корня, в то время как в другом находится только один из них; далее, ясно, что если два корня  $[\lambda], [\lambda']$  принадлежат одному и тому же периоду из  $f$  членов, то значение выражения  $\frac{\lambda'}{\lambda} \pmod{n}$  сравнимо с некоторой степенью числа  $h$ , т. е. что можно положить  $\lambda' \equiv \lambda g^{ve} \pmod{n}$ .

II. Если  $f = n - 1, e = 1$ , то период  $(f, 1)$ , очевидно, совпадает с  $\Omega$ ; во всех остальных случаях  $\Omega$  состоит из периодов  $(f, 1), (f, g), (f, g^2), \dots, (f, g^{e-1})$ . Поэтому эти периоды полностью различны, и ясно, что всякий другой однотипный период  $(f, \lambda)$  совпадает с одним из указанных, если только  $[\lambda]$  принадлежит к  $Q$ , т. е. если  $\lambda$  не делится на  $n$ . Период  $(f, 0)$  или  $(f, kn)$  состоит из  $f$  единиц. Точно так же легко видеть, что если  $\lambda$  является не делящимся на  $n$



числом, то совокупность  $e$  периодов  $(f, \lambda), (f, \lambda g), (f, \lambda g^2), \dots, (f, \lambda g^{e-1})$  совпадает с  $\Omega$ . Так, например, для  $n = 19$ ,  $f = 6$  совокупность  $\Omega$  состоит из трех периодов  $(6, 1), (6, 2), (6, 4)$ , и к любому из них может быть сведен любой другой, кроме  $(6, 0)$ .

III. Если  $n - 1$  есть произведение трех положительных чисел  $a, b, c$ , то очевидно, что каждый период из  $bc$  членов состоит из  $b$  периодов по  $c$  членов в каждом, а именно,  $(bc, \lambda)$  состоит из  $(c, \lambda), (c, \lambda g^a), (c, \lambda g^{2a}), \dots, (c, \lambda g^{ab-a})$ , вследствие чего последние называются содержащимися в первых. Так, например, для  $n = 19$  период  $(6, 1)$  состоит из трех периодов  $(2, 1), (2, 8), (2, 7)$ , первый из которых содержит корни  $r, r^{18}$ , второй — корни  $r^8, r^{11}$ , и третий — корни  $r^7, r^{12}$ .

## 345

**Теорема.** Пусть  $(f, \lambda), (f, \mu)$  суть два однотипных, совпадающих или различных периода, и пусть  $(f, \lambda)$  состоит из корней  $[\lambda], [\lambda'], [\lambda''], \dots$ . Тогда произведение  $(f, \lambda)$  и  $(f, \mu)$  является суммой  $f$  однотипных периодов, именно, равно

$$(f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \dots = W.$$

**Доказательство.** Пусть, как и раньше,  $n - 1 = ef$ ,  $g$  — первообразный корень по модулю  $n$  и  $h = g^e$ , так что, согласно предыдущему,  $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2) = \dots$ . Тогда искомое произведение равно

$$[\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] \cdot (f, \lambda h^2) + \dots,$$

т. е. равно

$$\begin{aligned} & [\lambda + \mu] + [\lambda h + \mu] + \dots + [\lambda h^{f-1} + \mu] + \\ & + [\lambda h + \mu h] + [\lambda h^2 + \mu h] + \dots + [\lambda h^f + \mu h] + \\ & + [\lambda h^2 + \mu h^2] + [\lambda h^3 + \mu h^2] + \dots + [\lambda h^{f+1} + \mu h^2] + \dots; \end{aligned}$$

последнее выражение всего содержит  $f^2$  корней. Если теперь сложить здесь отдельные вертикальные ряды, то мы, очевидно, получим

$$(f, \lambda + \mu) + (f, \lambda h + \mu) + \dots + (f, \lambda h^{f-1} + \mu),$$

и легко видеть, что это выражение совпадает с  $W$ , так как числа

$\lambda, \lambda', \lambda'', \dots$ , по предположению, сравнимы (в каком порядке — безразлично) по модулю  $n$  с числами  $\lambda, \lambda h, \lambda h^2, \dots, \lambda h^{f-1}$  и потому также числа

$$\lambda + \mu, \lambda' + \mu, \lambda'' + \mu, \dots$$

должны быть сравнимы с числами

$$\lambda + \mu, \lambda h + \mu, \lambda h^2 + \mu, \dots, \lambda h^{f-1} + \mu.$$

*К этой теореме мы добавим несколько дополнений.*

I. Если  $k$  обозначает некоторое целое число, то произведение  $(f, k\lambda)$  на  $(f, k\mu)$  равно

$$(f, k(\lambda + \mu)) + (f, k(\lambda' + \mu)) + (f, k(\lambda'' + \mu)) + \dots$$

II. Так как отдельные части, из которых состоит  $W$ , совпадают либо с суммой  $(f, 0)$ , которая равна  $f$ , либо с одной из сумм  $(f, 1), (f, g), (f, g^2), \dots, (f, g^{e-1})$ , то  $W$  можно привести к виду

$$W = af + b(f, 1) + b'(f, g) + b''(f, g^2) + \dots + b^{(e-1)}(f, g^{e-1}),$$

где коэффициенты  $a, b, b', \dots$  являются положительными целыми числами (некоторые из которых могут быть равны 0). Далее, ясно, что произведение  $(f, k\lambda)$  на  $(f, k\mu)$  равно

$$af + b(f, k) + b'(f, kg) + \dots + b^{(e-1)}(f, kg^{e-1}).$$

Например, для  $n = 19$  произведение суммы  $(6, 1)$  на себя же, т. е. квадрат этой суммы равен  $(6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = 6 + 2(6, 1) + (6, 2) + 2(6, 4)$ .

III. Так как произведение отдельных частей  $W$  и однотипного с рассмотренным выше периодом  $(f, \nu)$  может быть представлено в аналогичном виде, то ясно, что и произведение трех периодов  $(f, \lambda), (f, \mu), (f, \nu)$  представляется в виде  $cf + d(f, 1) + \dots + d^{(e-1)}(f, g^{e-1})$ , и что коэффициенты  $c, d, \dots$  будут целыми положительными числами (или равны 0), и, кроме того, для любого целого значения  $k$  имеет место

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = cf + d(f, k) + d'(f, kg) + \dots$$

Точно так же эта теорема может быть распространена на любое число однотипных периодов, причем безразлично, являются ли

эти периоды все различными или же они частично или полностью совпадают между собой.

IV. Из этого мы заключаем, что если в целой рациональной алгебраической функции  $F = \varphi(t, u, v, \dots)$  подставить вместо переменных  $t, u, v, \dots$  соответственно однотипные периоды  $(f, \lambda), (f, \mu), (f, \nu), \dots$ , то значение этой функции представится в виде

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) + \dots + B^{(e-1)}(f, g^{e-1}),$$

причем коэффициенты  $A, B, B', \dots$  все будут целыми числами, если являются целыми все постоянные коэффициенты у  $F$ ; если же вместо  $t, u, v, \dots$  подставить соответственно  $(f, k\lambda), (f, k\mu), (f, k\nu), \dots$ , то значение  $F$  примет вид  $A + B(f, k) + B'(f, kg) + \dots$ .

346

**Теорема.** *Предполагая, что  $\lambda$  есть не делящееся на  $n$  число и обозначая ради краткости  $(f, \lambda)$  через  $p$ , мы доказываем, что каждый другой однотипный с  $(f, \lambda)$  период  $(f, \mu)$ , где  $\mu$  также предполагается не делящимся на  $n$ , приводится к виду*

$$\alpha + \beta p + \gamma p^2 + \dots + \theta p^{e-1},$$

где коэффициенты  $\alpha, \beta, \dots$  являются определенными рациональными величинами.

**Доказательство.** Обозначим для краткости периоды  $(f, \lambda g), (f, \lambda g^2), (f, \lambda g^3), \dots, (f, \lambda g^{e-1})$ , число которых равно  $e - 1$  и с одним из которых обязательно совпадает период  $(f, \mu)$ , через  $p', p'', p''', \dots$ . Тогда мы тотчас же получаем равенство

(I) 
$$0 = 1 + p + p' + p'' + p''' + \dots$$

Если же мы по правилам предыдущего пункта вычислим значения степеней числа  $p$  до  $(e - 1)$ -й, то получим еще  $e - 2$  равенств вида

(II) 
$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \dots,$$

(III) 
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \dots,$$

(IV) 
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \dots,$$

. . . . .

где все коэффициенты  $A, a, a', \dots, B, b, b', \dots$  являются целыми числами и не зависят (что и само по себе очевидно, а также не-

посредственно следует из предыдущего пункта) от  $\lambda$ ; таким образом, указанные равенства остаются справедливыми, если вместо  $\lambda$  подставить любое другое значение; это замечание распространяется, очевидно, также и на равенство (I), если только считать  $\lambda$  не делящимся на  $n$ .

Положим  $(f, \mu) = p'$ , ибо легко видеть, что если  $(f, \mu), \dots$  совпадает с некоторым другим периодом из  $p'', p''', \dots$ , то все равно остаются применимыми следующие рассуждения. Так как число уравнений (I), (II), (III), ... равно  $e - 1$ , то величины  $p'', p''', \dots$ , число которых равно  $e - 2$ , могут быть при помощи известных методов отсюда исключены, после чего получится свободное от них уравнение вида

$$(Z) \quad 0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \dots + \mathfrak{M}p^{e-1} + \mathfrak{N}p',$$

причем можно попутно добиться того, что все коэффициенты  $\mathfrak{A}, \mathfrak{B}, \dots, \mathfrak{N}$  будут целыми числами, хотя бы одно из которых не равно нулю. Если теперь, например,  $\mathfrak{N}$  не равно 0, то отсюда тотчас же следует, что  $p'$  определяется именно тем способом, как утверждается в теореме. Таким образом, нам остается только доказать, что  $\mathfrak{N}$  не может быть равно 0.

Если мы предположим, что  $\mathfrak{N} = 0$ , то будет удовлетворяться уравнение  $(Z) : \mathfrak{M}p^{e-1} + \dots + \mathfrak{B}p + \mathfrak{A} = 0$ , — а так как его степень заведомо не может превосходить  $(e - 1)$ , то ему могут удовлетворять не более чем  $e - 1$  различных значений  $p$ . Но так как уравнения, из которых выведено уравнение  $(Z)$ , не зависят от  $\lambda$ , то ясно, что и  $(Z)$  не зависит от  $\lambda$ , т. е. сохраняется, какое бы вместо  $\lambda$  ни подставить целое не делящееся на  $n$  число. Поэтому уравнение  $(Z)$  будет удовлетворяться, какую бы сумму  $(f, 1), (f, g), (f, g^2), \dots, (f, g^{e-1})$  ни подставить вместо  $p$ , откуда сразу следует, что эти суммы не могут быть все различны, а что по крайней мере две из них должны быть равны. Пусть одна из этих равных сумм содержит корни  $[\zeta], [\zeta'], [\zeta''], \dots$ , а другая — корни  $[\eta], [\eta'], [\eta''], \dots$  предположим (это допустимо), что все числа  $\zeta, \zeta', \zeta'', \dots, \eta, \eta', \eta'', \dots$  положительны и меньше чем  $n$ ; очевидно, что они также будут все различны и не равны 0. Если функцию

$$x^\zeta + x^{\zeta'} + x^{\zeta''} + \dots - x^\eta - x^{\eta'} - x^{\eta''} - \dots,$$

старший член которой имеет степень не более высокую чем  $x^{n-1}$ , обозначить через  $Y$ , то, очевидно, при  $x = [1]$  будет иметь место  $Y = 0$ ; поэтому  $Y$  содержит сомножитель  $x - [1]$ , причем этот сомножитель будет у  $Y$  общим с той функцией, которую мы ранее обозначали через  $X$ . Но легко показать, что это невозможно. Действительно, если бы  $Y$  и  $X$  имели какой-нибудь общий сомножитель, то наибольший общий делитель функций  $X, Y$  (то что он имеет степень меньшую чем  $n$ , немедленно следует из того, что  $Y$  делится на  $x$ ) имел бы сплошь рациональные коэффициенты, что сразу вытекает из природы операций, при помощи которых находится наибольший общий делитель двух функций, все коэффициенты которых рациональны. Однако в п. 341 мы показали, что  $X$  не может содержать сомножителей степени ниже  $n - 1$ , все коэффициенты которых рациональны. Следовательно, предположение, что  $\mathfrak{N} = 0$ , не может быть правильным.

**Пример.** Для  $n = 19$ ,  $f = 6$  будет  $p^2 = 6 + 2p + p' + 2p''$ ; отсюда и из  $0 = 1 + p + p' + p''$  мы находим, что  $p' = 4 - p^2$ ,  $p'' = -5 - p + p^2$ ; следовательно,

$$\begin{aligned} (6, 2) &= 4 - (6, 1)^2, & (6, 4) &= -5 - (6, 1) + (6, 1)^2, \\ (6, 4) &= 4 - (6, 2)^2, & (6, 1) &= -5 - (6, 2) + (6, 2)^2, \\ (6, 1) &= 4 - (6, 4)^2, & (6, 2) &= -5 - (6, 4) + (6, 4)^2. \end{aligned}$$

### 347

**Теорема.** Если  $F = \varphi(t, u, v, \dots)$  есть симметрическая\* целая рациональная алгебраическая функция от  $f$  переменных  $t, u, v, \dots$ , и если в нее вместо этих переменных подставить  $f$  корней, содержащихся в периоде  $(f, \lambda)$ , то значение  $F$ , в соответствии с п. 340,

---

\* Симметрическими функциями, как известно, называются такие функции, которые содержат все переменные одинаковым образом, или, точнее, которые не меняются, как бы мы не переставляли между собой переменные; такими функциями являются, например, сумма всех переменных, произведение всех переменных, сумма всевозможных попарных произведений переменных и т. д.

можно представить в виде

$$A + A' [1] + A'' [2] + \dots = W.$$

Тогда корни, которые в этом выражении принадлежат одному и тому же периоду из  $f$  членов, будут иметь равные коэффициенты.

**Доказательство.** Пусть  $[p]$ ,  $[q]$  — два корня, принадлежащие одному и тому же периоду и пусть  $p$ ,  $q$  положительны и меньше чем  $n$ ; тогда нужно доказать, что  $[p]$  и  $[q]$  имеют в выражении для  $W$  одинаковые коэффициенты. Пусть  $q \equiv pg^{ve} \pmod{n}$ ; далее, пусть содержащиеся в  $(f, \lambda)$  корни суть  $[\lambda]$ ,  $[\lambda']$ ,  $[\lambda'']$ , ..., где числа  $\lambda$ ,  $\lambda'$ ,  $\lambda''$ , ... предполагаются положительными и меньшими чем  $n$ ; наконец, пусть наименьшие положительные вычеты чисел  $\lambda g^{ve}$ ,  $\lambda' g^{ve}$ ,  $\lambda'' g^{ve}$ , ... по модулю  $n$  суть соответственно  $\mu$ ,  $\mu'$ ,  $\mu''$ , ..., эти числа, очевидно, совпадают с числами  $\lambda$ ,  $\lambda'$ ,  $\lambda''$ , ..., только взятыми в другом порядке. Тогда из п. 340 вытекает, что выражение

$$\varphi([\lambda g^{ve}], [\lambda' g^{ve}], [\lambda'' g^{ve}], \dots) = (I)$$

принимает вид

$A + A' [g^{ve}] + A'' [2g^{ve}] + \dots$ , или  $A + A' [\theta'] + A'' [\theta''] + \dots = (W')$ , где  $\theta'$ ,  $\theta''$ , ... обозначают наименьшие вычеты чисел  $g^{ve}$ ,  $2g^{ve}$ , ... по модулю  $n$ , откуда видно, что  $[q]$  имеет в  $[W']$  такой же коэффициент, что и  $[p]$  в  $[W]$ . Но легко видеть, что при раскрытии выражения  $(I)$  получается тот же результат, что и при раскрытии выражения  $\varphi([\mu], [\mu'], [\mu''], \dots)$ , так как  $\mu \equiv \lambda g^{ve}$ ,  $\mu' \equiv \lambda' g^{ve}$ , ...; а последнее выражение в свою очередь дает такой же результат, как и  $\varphi([\lambda], [\lambda'], [\lambda''], \dots)$ , так как  $\mu$ ,  $\mu'$ ,  $\mu''$ , ... отличаются от  $\lambda$ ,  $\lambda'$ ,  $\lambda''$ , ... только порядком расположения, а для симметрической функции это не имеет значения. Отсюда мы заключаем, что  $W'$  полностью совпадает с  $W$ , так что корень  $[q]$  имеет в  $W$  тот же коэффициент, что и  $[p]$ .

Поэтому  $W$ , очевидно, может быть представлено в виде

$$A + a(f, 1) + a'(f, g) + a''(f, g^2) + \dots + a^{(e-1)}(f, g^{e-1}),$$

где коэффициенты  $A$ ,  $a$ , ...,  $a^{(e-1)}$  являются определенными величинами, которые, кроме того, будут целыми числами, если являются целыми все рациональные коэффициенты у  $F$ . Так, например, если

$n = 19$ ,  $f = 6$ ,  $\lambda = 1$ , и  $\varphi$  обозначает сумму всевозможных попарных произведений переменных, то значение  $\varphi$  можно представить в виде  $3 + (6, 1) + (6, 4)$ .

Далее, легко видеть, что если мы затем подставим вместо  $t$ ,  $u$ ,  $v$ , ... корни из другого периода  $(f, k\lambda)$ , то значение  $F$  будет равно  $A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \dots$

## 348

Так как у каждого уравнения

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} + \dots = 0$$

коэффициенты  $\alpha$ ,  $\beta$ ,  $\gamma$ , ... являются симметричными функциями корней, а именно,  $\alpha$  — суммой всех корней,  $\beta$  — суммой всевозможных произведений корней по два,  $\gamma$  — суммой всевозможных их произведений по три и т. д., то в уравнении, корнями которого являются корни, содержащиеся в периоде  $(f, \lambda)$ , первый коэффициент равен  $(f, \lambda)$ , в то время как каждый из остальных может быть представлен в виде

$$A + a(f, 1) + a'(f, g) + \dots + a^{(e-1)}(f, g^{e-1}),$$

где все числа  $A$ ,  $a$ ,  $a'$ , ... целые; и, кроме того, ясно, что уравнение, корнями которого являются корни, содержащиеся в некотором другом периоде  $(f, k\lambda)$ , получается из указанного уравнения, если заменить в нем коэффициент  $(f, 1)$  на  $(f, k)$ ,  $(f, g)$  — на  $(f, kg)$ , и вообще  $(f, p)$  — на  $(f, kp)$ . Таким образом, можно указать  $e$  уравнений  $z = 0$ ,  $z' = 0$ ,  $z'' = 0$ , ..., корнями которых являются корни, содержащиеся соответственно в  $(f, 1)$ ,  $(f, g)$ ,  $(f, g^2)$ , ..., если только известно  $e$  сумм  $(f, 1)$ ,  $(f, g)$ ,  $(f, g^2)$ , ..., или даже если найдена только одна из этих сумм, так как, согласно п. 346, по одной из них можно при помощи рациональных операций определить и все остальные. При этом мы одновременно получаем разложение функции  $X$  на  $e$  сомножителей степени  $f$ ; действительно, произведение функций  $z$ ,  $z'$ ,  $z''$ , ..., очевидно, равно  $X$ .

**Пример.** Для  $n = 19$  сумма всех корней из периода  $(6, 1)$  равна  $(6, 1) = \alpha$ ; сумма произведений этих корней по два будет равна

$3 + (6, 1) + (6, 4) = \beta$ ; аналогично находим, что сумма произведений корней по три равна  $2 + 2(6, 1) + (6, 2) = \gamma$ , сумма произведений корней по четыре равна  $3 + (6, 1) + (6, 4) = \delta$ , сумма произведений корней по пять равна  $(6, 1) = \varepsilon$ , и произведение всех корней равно 1. Тем самым уравнение

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0$$

охватывает все корни, содержащиеся в  $(6, 1)$ . Если теперь в коэффициентах  $\alpha, \beta, \gamma, \dots$  вместо  $(6, 1), (6, 2), (6, 3)$  подставить соответственно  $(6, 2), (6, 4), (6, 1)$ , то получится уравнение  $z' = 0$ , которое охватывает корни, содержащиеся в  $(6, 2)$ , а если проделать такую же перестановку еще раз, то получится уравнение  $z'' = 0$ , которое будет охватывать корни, содержащиеся в  $(6, 4)$ , и произведение  $zz'z''$  будет равно  $X$ .

### 349

В большинстве случаев, особенно, когда  $f$  — большое число, удобнее находить коэффициенты  $\alpha, \beta, \gamma, \dots$  при помощи теоремы Ньютона из сумм степеней корней. Именно, непосредственно ясно, что сумма квадратов корней, содержащихся в  $(f, \lambda)$ , равна  $(f, 2\lambda)$ , сумма кубов равна  $(f, 3\lambda)$  и т. д. Поэтому, если ради краткости вместо  $(f, \lambda), (f, 2\lambda), (f, 3\lambda), \dots$  писать соответственно  $q, q', q'', \dots$ , то

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'', \dots,$$

причем произведения из двух периодов, согласно п. 345, тотчас же должны быть преобразованы в суммы периодов. Так, в нашем примере, если вместо  $(6, 1), (6, 2), (6, 4)$  написать соответственно  $p, p', p''$ , то величины  $q, q', q'', q''', q'''', q'''''$  будут соответственно равны  $p, p' p', p'', p', p''$ ; поэтому

$$\begin{aligned} \alpha &= p, \\ 2\beta &= p^2 - pp' = 6 + 2p + 2p'', \\ 3\gamma &= (3 + p + p'')p - pp' + p' = 6 + 6p + 3p', \\ 4\delta &= (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p'', \end{aligned}$$

и т. д.



Заметим, что таким способом нам нужно вычислять только половину коэффициентов; действительно, не трудно доказать, что коэффициенты, равноудаленные от концов, равны, именно, последний коэффициент равен 1; предпоследний равен  $\alpha$ , третий от конца равен  $\beta$  и т. д., т. е. последние коэффициенты получаются из первых заменой  $(f, 1)$ ,  $(f, g), \dots$  на  $(f, -1)$ ,  $(f, -g), \dots$  или на  $(f, n-1)$ ,  $(f, n-g), \dots$ . Первый случай имеет место, когда  $f$  четно, а второй, когда  $f$  нечетно; последний же коэффициент всегда равен 1. Доказательство этого факта основывается на теореме п. 79; однако, ради краткости, мы не будем здесь на нем останавливаться.

## 350

**Теорема.** Пусть  $n-1$  есть произведение трех целых положительных чисел  $\alpha, \beta, \gamma$ ; пусть, далее, период  $(\beta\gamma, \lambda)$ , который имеет  $\beta\gamma$  членов, состоит из  $\beta$  меньших периодов, имеющих по  $\gamma$  членов, именно из  $(\gamma, \lambda), (\gamma, \lambda'), (\gamma, \lambda''), \dots$ ; предположим еще, что если в некоторой функции от  $\beta$  переменных, обладающей свойством, указанным в п. 347, именно, в функции  $F = \varphi(t, u, v, \dots)$ , вместо переменных  $t, u, v, \dots$  подставить соответственно суммы  $(\gamma, \lambda), (\gamma, \lambda'), (\gamma, \lambda''), \dots$ , то значение функции приводится по правилам из п. 345, IV к виду  $A + a(\gamma, 1) + a'(\gamma, g) + \dots + a^{(\xi)}(\gamma, g^{\alpha\beta-\alpha}) + \dots + a^{(\theta)}(\gamma, g^{\alpha\beta-1}) \equiv W$ . Тогда я утверждаю, что если  $F$  есть симметрическая функция, то те периоды в  $W$ , которые содержатся в одном и том же периоде из  $\beta\gamma$  членов, т. е., вообще, периоды вида  $(\gamma, g^\mu)$  и  $(\gamma, g^{\alpha\nu+\mu})$ , где  $\nu$  обозначает некоторое целое число, будут иметь одинаковые коэффициенты.

**Доказательство.** Так как периоды  $(\beta\gamma, \lambda g^\alpha)$  и  $(\beta\gamma, \lambda)$  совпадают, то меньшие периоды  $(\gamma, \lambda g^\alpha); (\gamma, \lambda' g^\alpha), (\gamma, \lambda'' g^\alpha), \dots$  из которых, очевидно, состоит первый период, будут обязательно совпадать с теми, из которых состоит другой период, лишь расположенными в другом порядке. Если, таким образом, предположить, что после того как первые подставлены вместо  $t, u, v, \dots$ , функция  $F$  переходит в  $W'$ , то  $W'$  будет совпадать с  $W$ . Но, согласно п. 347,

$$\begin{aligned} W' &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) + \dots + a^{(\xi)}(\gamma, g^{\alpha\beta}) + \dots + a^{(\theta)}(\gamma, g^{\alpha\beta+\alpha-1}) = \\ &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) + \dots + a^{(\xi)}(\gamma, 1) + \dots + a^{(\theta)}(\gamma, g^{\alpha-1}). \end{aligned}$$

При этом, так как это выражение должно совпадать с  $W$ , то первый, второй, третий и т. д. коэффициент у  $W$  (считая от  $a$ ) обязательно совпадает с  $(\alpha + 1)$ -м,  $(\alpha + 2)$ -м,  $(\alpha + 3)$ -м и т. д., откуда легко заключить, что, вообще, коэффициенты периодов  $(\gamma, g^\mu)$ ,  $(\gamma, g^{\alpha+\mu})$ ,  $(\gamma, g^{2\alpha+\mu})$ , ...,  $(\gamma, g^{\nu\alpha+\mu})$ , которые стоят на  $(\mu + 1)$ -м,  $(\alpha + \mu + 1)$ -м,  $(2\alpha + \mu + 1)$ -м, ...,  $(\nu\alpha + \mu + 1)$ -м месте, должны совпадать между собой. Это и требовалось доказать.

Из этого вытекает, что  $W$  можно привести к виду

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \dots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}),$$

где все коэффициенты  $A, a, \dots$  будут целыми числами, если являются целыми все постоянные коэффициенты у  $F$ . Далее, легко видеть, что если после этого подставить в функцию  $F$ , вместо переменных,  $\beta$  периодов (состоящих из  $\gamma$  членов), которые содержатся в другом периоде из  $\beta\gamma$  членов, например, в  $(\beta\gamma, \lambda k)$ , и которые тогда суть, очевидно,  $(\gamma, \lambda k)$ ,  $(\gamma, \lambda' k)$ ,  $(\gamma, \lambda'' k)$ , ..., то получающееся при этом значение будет иметь вид

$$A + a(\beta\gamma, k) + a'(\beta\gamma, gk) + \dots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1} k).$$

Далее ясно, что теорема остается верной и в том случае, когда  $\alpha = 1$ , т. е.  $\beta\gamma = n - 1$ ; именно, здесь все коэффициенты у  $W$  равны и потому  $W$  приводится к виду  $A + a(\beta\gamma, 1)$ .

### 351

Итак, если мы сохраним все обозначения предыдущего пункта, то ясно, что отдельные коэффициенты уравнения, корнями которого являются  $\beta$  сумм  $(\gamma, \lambda)$ ,  $(\gamma, \lambda')$ ,  $(\gamma, \lambda'')$ , ..., могут быть представлены в виде

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \dots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}),$$

и что все числа  $A, a, \dots$  будут целыми, а уравнение, корнями которого служат  $\beta$  периодов из  $\gamma$  членов, содержащиеся в некотором другом периоде  $(\beta\gamma, k\lambda)$ , получается из первого уравнения, если всюду в его коэффициентах вместо каждого периода  $(\beta\gamma, \mu)$  подставить  $(\beta\gamma, k\mu)$ . Если, таким образом,  $\alpha = 1$ , то все  $\beta$  периодов из  $\gamma$

членов определяются уравнением  $\beta$ -й степени, отдельные коэффициенты которого приводятся к виду  $A + a(\beta\gamma, 1)$  и поэтому являются известными величинами, так как  $(\beta\gamma, 1) = (n - 1, 1) = -1$ . Если же  $\alpha > 1$ , то коэффициенты уравнения, корнями которого являются все периоды из  $\beta\gamma$  членов, содержащиеся в некотором заданном периоде из  $\gamma$  членов, будут известны, как только будут известны численные значения всех  $\alpha$  периодов из  $\beta\gamma$  членов. Впрочем, часто, особенно когда  $\beta$  не очень мало, вычисление коэффициентов этих уравнений удобнее производить, находя сначала суммы степеней корней, и уже из них так же, как в п. 349, получать при помощи теоремы Ньютона значения коэффициентов.

**Пример I.** Найдем для  $n = 19$  уравнение, корнями которого являются суммы  $(6, 1)$ ,  $(6, 2)$ ,  $(6, 4)$ . Если мы обозначим эти корни соответственно через  $p, p', p''$ , а искомое уравнение через

$$x^3 - Ax^2 + Bx - C = 0,$$

то

$$A = p + p' + p'', B = pp' + pp'' + p'p'', C = pp'p''.$$

Поэтому

$$A = (18, 1) = -1;$$

далее мы имеем

$$pp' = p + 2p' + 3p'', pp'' = 2p + 3p' + p'', p'p'' = 3p + p' + 2p'',$$

и потому

$$B = 6(p + p' + p'') = 6(18, 1) = -6;$$

наконец,

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7.$$

Поэтому искомым уравнением является

$$x^3 + x^2 - 6x - 7 = 0.$$

Если мы применим здесь другой метод, то получим

$$p + p' + p'' = -1,$$

$$p^2 = 6 + 2p + p' + 2p'', p'^2 = 6 + 2p' + p'' + 2p, p''^2 = 6 + 2p'' + p + 2p',$$

поэтому

$$p^2 + p'^2 + p''^2 = 18 + 5(p + p' + p'') = 13,$$

и точно так же

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2.$$

Отсюда при помощи теоремы Ньютона мы получим то же уравнение, что и перед этим.

II. Найдем для  $n = 19$  уравнение, корнями которого являются суммы  $(2, 1)$ ,  $(2, 7)$ ,  $(2, 8)$ . Если обозначить их соответственно через  $q, q', q''$ , то мы найдем

$q + q' + q'' = (6, 1)$ ,  $qq' + qq'' + q'q'' = (6, 1) + (6, 4)$ ,  $qq'q'' = 2 + (6, 2)$ ; поэтому, если сохранить обозначения предыдущего пункта, то искомого уравнение запишется в виде

$$x^3 - px^2 + (p + p'')x - 2 - p' = 0.$$

Уравнение, корнями которого являются содержащиеся в  $(6, 2)$  суммы  $(2, 2)$ ,  $(2, 3)$ ,  $(2, 5)$ , получается из предыдущего, если вместо  $p, p', p''$  подставить соответственно  $p', p'', p$ , а если эту же подстановку произвести еще раз, то получится уравнение, корнями которого являются содержащиеся в  $(6, 4)$  суммы  $(2, 4)$ ,  $(2, 6)$ ,  $(2, 9)$ .

**На предыдущих исследованиях  
основывается решение уравнения  $X = 0$**

352

Предыдущие теоремы вместе с указанными следствиями из них содержат основные пункты всей теории, и метод нахождения корней  $\Omega$  может быть изложен теперь в немногих словах.

Прежде всего нужно выбрать число  $g$ , которое является по модулю  $n$  первообразным корнем, и найти наименьшие вычеты степеней  $g$  до  $g^{n-2}$  по модулю  $n$ . Разложим  $n - 1$  на множители, причем, если желательно свести проблему к уравнениям по возможности более низкой степени, то на простые; пусть эти сомножители (в совершенно произвольном порядке) суть  $\alpha, \beta, \gamma, \dots, \zeta$ ; положим

$$\frac{n-1}{\alpha} = \beta\gamma\dots\zeta = a, \quad \frac{n-1}{\alpha\beta} = \gamma\dots\zeta = b, \dots$$

Разобьем все корни из  $\Omega$  на  $\alpha$  периодов из  $a$  членов, каждый из них снова разобьем на  $\beta$  периодов из  $b$  членов, каждый из них

снова на  $\gamma$  периодов и т. д. Найдем в соответствии с предыдущим пунктом уравнение (A) степени  $\alpha$ , корнями которого являются указанные  $\alpha$  сумм по  $a$  членов; тем самым значения указанных сумм станут известными после решения этого уравнения.

Однако здесь возникает одна трудность, так как представляется неясным, какой из корней уравнения (A) приравнивать каждой сумме, т. е. какой корень следует обозначить через  $(a, 1)$ , какой через  $(a, g), \dots$ . Это затруднение можно обойти следующим образом. Через  $(a, 1)$  можно обозначить любой корень уравнения (A); действительно, так как каждый корень этого уравнения является суммой  $a$  корней из  $\Omega$ , причем совершенно безразлично, какой именно корень из  $\Omega$  обозначен через [1], то можно, очевидно, предположить, что через [1] обозначен какой-то из тех корней, из которых состоит заданный корень уравнения (A), вследствие чего этот корень будет равен  $(a, 1)$ . Однако этим корень [1] будет определен еще не вполне, так как остается еще совершенно неопределенным, какой именно корень из тех, что образуют  $(a, 1)$ , мы берем в качестве [1]. Но если сама сумма  $(a, 1)$  определена, то из нее уже могут быть получены все остальные суммы из  $a$  членов (п. 346). Отсюда тотчас же вытекает, что при решении указанного уравнения нам достаточно найти только какой-нибудь один корень.

Для этой же цели можно применить и следующий, менее прямой, метод. Возьмем в качестве [1] некоторый определенный корень, т. е. положим  $[1] = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$ , где целое число  $k$  выбрано произвольно, однако так, что оно не делится на  $n$ ; тогда и [2], [3], ... тоже будут определенными корнями, а потому и суммы  $(a, 1)$ ,  $(a, g), \dots$  будут определенными величинами. Если вычислить их по таблице синусов с весьма незначительной точностью, именно с такой, чтобы только иметь возможность судить, какая из них больше, а какая меньше, то уже не останется никакой неопределенности в вопросе о том, как обозначать отдельные корни уравнения (A).

После того как найдены все  $\alpha$  сумм из  $a$  членов, найдем, в соответствии с предыдущим пунктом, уравнение (B) степени  $\beta$ , корнями которого являются  $\beta$  сумм из  $b$  членов, которые встречаются в  $(a, 1)$ ; все коэффициенты этого уравнения будут известны

Так как еще остается произвольным, который из  $a = \beta b$  корней, содержащихся в  $(a, 1)$ , обозначить через [1], то любой корень уравнения  $(B)$  можно обозначить через  $(b, 1)$ , ибо, очевидно, можно предположить, что в качестве [1] был выбран некоторый из  $b$  корней этого уравнения. Итак, найдем посредством решения уравнения  $(B)$  какой-нибудь *один* его корень, обозначим его через  $(b, 1)$  и получим отсюда, в соответствии с п. 346, все остальные суммы из  $b$  членов. Одновременно мы имеем при этом критерий правильности вычислений, так как всегда те суммы из  $b$  членов, которые принадлежат одному и тому же периоду из  $a$  членов, должны давать известные суммы.

Во многих случаях так же просто было бы найти  $\alpha - 1$  остальных уравнений  $\beta$ -й степени, корнями каждого из которых являются  $\beta$  сумм из  $b$  членов, которые содержатся в других периодах  $(a, g)$ ,  $(a, g^2), \dots$  из  $a$  членов, и посредством решения отыскать *все* корни как этих уравнений, так и уравнения  $(B)$ ; однако тогда, так же, как и выше, пришлось бы прибегнуть к помощи таблицы синусов, чтобы определить, каким именно периодам из  $b$  членов должны быть приравнены отдельные полученные таким способом корни. Впрочем, для этой цели можно применить и много других приемов, изложить которые полностью здесь мы не можем; лишь для случая  $\beta = 2$  мы продемонстрируем один прием, который особенно важен и легче может быть пояснен на примере, чем при помощи теоретических рассуждений.

После того как таким путем найдены значения всех  $\alpha\beta$  сумм из  $b$  членов, из них совершенно таким же способом при помощи уравнений  $\gamma$ -й степени могут быть получены все  $\alpha\beta\gamma$  сумм из  $c$  членов. Именно, можно либо получить, согласно п. 350, только одно уравнение  $\gamma$ -й степени, корнями которого являются  $\gamma$  содержащихся в  $(b, 1)$  сумм из  $c$  членов, затем найти *один* его корень, положить его равным  $(c, 1)$  и, наконец, получить отсюда, в соответствии с п. 346, все остальные подобные суммы, либо же нужно получить все  $\alpha\beta$  уравнений  $\gamma$ -й степени, корнями каждого из которых являются  $\gamma$  сумм из  $c$  членов, каждая из которых содержится в отдельном периоде из  $b$  членов, затем решением этих уравнений найти значения всех корней, и, наконец, определить

порядок их расположения так же, как и выше, при помощи таблицы синусов или же посредством приема, иллюстрируемого приведенными ниже примерами для  $\gamma = 2$ .

Продолжая таким же образом, мы, очевидно, в конце концов получим все  $(n - 1)/\zeta$  сумм из  $\zeta$  членов; если же получить, в соответствии с п. 348, уравнение степени  $\zeta$ , корнями которого являются  $\zeta$  содержащихся в  $(\zeta, 1)$  корней из  $\Omega$ , то все коэффициенты этого уравнения будут известными величинами; если при решении его мы найдем какой-нибудь один корень, то его можно будет положить равным [1], и все остальные корни из  $\Omega$  будут его степенями. Если угодно, можно, решив указанное уравнение, получить также и все его корни, а затем, решая  $\frac{n-1}{\zeta} - 1$  других уравнений  $\zeta$ -степени, корнями каждого из которых являются  $\zeta$  корней, содержащихся в отдельных периодах из  $\zeta$  членов, найти и все остальные корни из  $\Omega$ .

Отметим, что после того как решено первое уравнение (A), т. е. получены значения всех  $\alpha$  сумм из  $a$  членов, тем самым немедленно получается разложение функции  $X$  на  $\alpha$  сомножителей степени  $a$  в соответствии с п. 348, и, далее, после решения уравнения (B), т. е. после нахождения значений всех  $\alpha\beta$  сумм из  $b$  членов, каждый из указанных сомножителей в свою очередь распадается на  $\beta$  сомножителей, т. е.  $X$  распадается на  $\alpha\beta$  сомножителей степени  $b$ , и т. д.

### 353

**Первый пример для  $n = 19$ .** Так как здесь  $n - 1 = 3 \cdot 3 \cdot 2$ , то получение корней  $\Omega$  сводится к решению двух кубических и одного квадратного уравнений. Этот пример понять будет особенно легко благодаря тому, что необходимые операции в большинстве случаев уже встречались ранее. Если в качестве первообразного корня взять число 2, то его степени будут иметь следующие наименьшие вычеты (показатели степеней написаны в первом ряду, а наименьшие вычеты во втором ряду под ними):

|   |   |   |   |    |    |   |    |   |    |    |    |    |    |    |    |    |     |
|---|---|---|---|----|----|---|----|---|----|----|----|----|----|----|----|----|-----|
| 0 | 1 | 2 | 3 | 4  | 5  | 6 | 7  | 8 | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17  |
| 1 | 2 | 4 | 8 | 16 | 13 | 7 | 14 | 9 | 18 | 17 | 15 | 11 | 3  | 6  | 12 | 5  | 10. |

Отсюда мы, в соответствии с пп. 344, 345, легко находим следующее разбиение всех корней из  $\Omega$  на три периода, состоящих каждый из шести членов, причем эти периоды в свою очередь распадаются каждый на три периода, состоящих из двух членов:

$$\Omega = (18, 1) \left\{ \begin{array}{l} (6, 1) \left\{ \begin{array}{l} (2, 1) \dots [1], [18] \\ (2, 8) \dots [8], [11] \\ (2, 7) \dots [7], [12] \end{array} \right. \\ (6, 2) \left\{ \begin{array}{l} (2, 2) \dots [2], [17] \\ (2, 16) \dots [3], [16] \\ (2, 14) \dots [5], [14] \end{array} \right. \\ (6, 4) \left\{ \begin{array}{l} (2, 4) \dots [4], [15] \\ (2, 13) \dots [6], [13] \\ (2, 19) \dots [9], [10]. \end{array} \right. \end{array} \right.$$

Уравнение (A), корнями которого являются суммы  $(6, 1)$ ,  $(6, 2)$ ,  $(6, 4)$ , есть

$$x^3 + x^2 - 6x - 7 = 0;$$

один из его корней приближенно равен  $-1,2218761623$ . Если взять его в качестве  $(6, 1)$ , то

$$(6, 2) = 4 - (6, 1)^2 \approx 2,5070186441,$$

$$(6, 4) = -5 - (6, 1) + (6, 1)^2 \approx -2,2851424818.$$

После этого  $X$  распадется на три сомножителя шестой степени, которые можно найти в соответствии с п. 348.

В качестве уравнения (B), корнями которого являются суммы  $(2, 1)$ ,  $(2, 7)$ ,  $(2, 8)$ , получается следующее уравнение:

$$x^3 - (6, 1)x^2 + [(6, 1) + (6, 4)]x - 2 - (6, 2) = 0,$$

или, приближенно,

$$x^3 + 1,2218761623x^2 - 3,5070186441x - 4,5070186441 = 0;$$

находим, что один корень  $\approx -1,3545631433$ ; обозначим его через  $(2, 1)$ . Но при помощи метода п. 346 мы находим следующие уравнения, где ради краткости вместо  $(2, 1)$  написано  $q$ :

$$(2, 2) = q^2 - 2; \quad (2, 3) = q^3 - 3q;$$

$$(2, 4) = q^4 - 4q^2 + 2;$$

$$(2, 5) = q^5 - 5q^3 + 5q;$$



$$\begin{aligned}(2, 6) &= q^6 - 6q^4 + 9q^2 - 2; \quad (2, 7) = q^7 - 7q^5 + 14q^3 - 7q; \\ (2, 8) &= q^8 - 8q^6 + 20q^4 - 16q^2 + 2; \\ (2, 9) &= q^9 - 9q^7 + 27q^5 - 30q^3 + 9q.\end{aligned}$$

Удобнее, чем по правилам п. 346, эти уравнения в данном случае могут быть получены посредством следующих рассуждений. Положим

$$[1] = \cos \frac{kP}{19} + i \sin \frac{kP}{19};$$

тогда

$$\begin{aligned}[18] &= \cos \frac{18kP}{19} + i \sin \frac{18kP}{19} = \cos \frac{kP}{19} - i \sin \frac{kP}{19}, \quad \text{и поэтому } (2, 1) = \\ &= 2 \cos \frac{kP}{19}; \quad \text{точно так же и вообще } [\lambda] = \cos \frac{\lambda kP}{19} + i \sin \frac{\lambda kP}{19} \text{ и по-} \\ \text{тому } (2, \lambda) &= [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2 \cos \frac{\lambda kP}{19}.\end{aligned}$$

Поэтому, если  $\frac{q}{2} = \cos \omega$ , то  $(2, 2) = 2 \cos 2\omega$ ,  $(2, 3) = 2 \cos 3\omega$ , и т. д., откуда по известным формулам для косинусов кратных углов выводятся те же формулы, что и выше. Из последних формул мы получаем следующие численные значения:

$$\begin{array}{l|l}(2, 2) \approx -0,1651586909 & (2, 6) \approx 0,4909709743 \\ (2, 3) \approx 1,5782810188 & (2, 7) \approx -1,7589475024 \\ (2, 4) \approx -1,9727226068 & (2, 8) \approx 1,8916344834 \\ (2, 5) \approx 1,0938963162 & (2, 9) \approx -0,8033908493\end{array}$$

Значения  $(2, 7)$ ,  $(2, 8)$  могут быть также выведены из уравнения (B), для которого эти значения являются двумя остальными корнями, причем вопрос о том, который из них есть  $(2, 7)$ , а который  $(2, 8)$ , может быть решен либо приближенным вычислением по указанным перед этим формулам, либо при помощи таблицы синусов, которая уже при самом поверхностном ее использовании показывает, что  $(2, 1) = 2 \cos \omega$ , если положить  $\omega = \frac{7}{19}P$ , вследствие чего

$$(2, 7) = 2 \cos \frac{49P}{19} = 2 \cos \frac{8P}{19} \quad \text{и} \quad (2, 8) = 2 \cos \frac{56P}{19} = 2 \cos \frac{P}{19}.$$

Точно так же можно найти суммы  $(2, 2)$ ,  $(2, 3)$ ,  $(2, 5)$  из уравнения

$$x^3 - (6, 2) x^2 + [(6, 1) + (6, 2)] x - 2 - (6, 4) = 0,$$

корнями которого они являются, и сомнение в том, какие корни надо положить равными каким из указанных сумм, разрешается точно таким же образом, как и перед этим; и подобно этому при помощи уравнения

$$x^3 - (6, 4) x^2 + [(6, 2) + (6, 4)] x - 2 - (6, 1) = 0$$

могут быть найдены суммы  $(2, 4)$ ,  $(2, 6)$   $(2, 9)$ .

Наконец,  $[1]$  и  $[18]$  являются корнями уравнения

$$x^2 - (2, 1) x + 1 = 0,$$

причем один из них равен  $\frac{1}{2}(2, 1) + i\sqrt{1 - \frac{1}{4}(2, 1)^2} = \frac{1}{2}(2, 1) + i\sqrt{\frac{1}{2} - \frac{1}{4}(2, 2)}$ , а другой равен  $\frac{1}{2}(2, 1) - i\sqrt{\frac{1}{2} - \frac{1}{4}(2, 2)}$ , откуда получается, что их численные значения приближенно равны  $-0,6772815716 \pm 0,7357239107i$ .

Шестнадцать остальных значений могут быть найдены либо посредством возведения в степень одного из этих двух корней, либо посредством решения восьми других подобных уравнений; применяя первый метод, нужно либо по таблице синусов, либо при помощи поясняемого на следующем примере способа выявить, для какого из двух корней мнимая часть имеет положительный знак, а для какого отрицательный. Таким способом находятся следующие значения, причем верхний знак соответствует первому, а нижний — второму корню:

$$[1] \text{ и } [18] \approx -0,6772815716 \pm 0,7357239107i,$$

$$[2] \text{ и } [17] \approx -0,0825793455 \mp 0,9965844930i.$$

$$[3] \text{ и } [16] \approx 0,7891405094 \pm 0,6142127127i,$$

$$[4] \text{ и } [15] \approx -0,9863613034 \pm 0,1645945903i,$$

$$[5] \text{ и } [14] \approx 0,5469481581 \mp 0,8371664783i,$$

$$[6] \text{ и } [13] \approx 0,2454854871 \pm 0,9694002659i,$$

$$[7] \text{ и } [12] \approx -0,8794737512 \mp 0,4759473930i,$$

$$[8] \text{ и } [11] \approx 0,9458172417 \mp 0,3246994692i,$$

$$[9] \text{ и } [10] \approx -0,4016954247 \pm 0,9157733267i.$$

Второй пример для  $n = 17$ . Здесь мы имеем  $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ , так что вычисление корней из  $\Omega$  сводится к решению четырех квадратных уравнений. В качестве первообразного корня мы возьмем здесь число 3, степени которого имеют по модулю 17 следующие вычеты:

|   |   |   |    |    |   |    |    |    |    |    |    |    |    |    |    |
|---|---|---|----|----|---|----|----|----|----|----|----|----|----|----|----|
| 0 | 1 | 2 | 3  | 4  | 5 | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8  | 7  | 4  | 12 | 2  | 6  |

Отсюда получаются следующие разбиения совокупности  $\Omega$  на два периода по восемь членов, четыре периода по четыре члена, восемь периодов по два члена:

$$\Omega = (16, 1) \left\{ \begin{array}{l} (8, 1) \left\{ \begin{array}{l} (4, 1) \left\{ \begin{array}{l} (2, 1) \cdot \cdot \cdot [1], [16] \\ (2, 13) \cdot \cdot \cdot [4], [13] \end{array} \right. \\ (4, 9) \left\{ \begin{array}{l} (2, 9) \cdot \cdot \cdot [8], [9] \\ (2, 15) \cdot \cdot \cdot [2], [15] \end{array} \right. \end{array} \right. \\ (8, 3) \left\{ \begin{array}{l} (4, 3) \left\{ \begin{array}{l} (2, 3) \cdot \cdot \cdot [3], [14] \\ (2, 5) \cdot \cdot \cdot [5], [12] \end{array} \right. \\ (4, 10) \left\{ \begin{array}{l} (2, 10) \cdot \cdot \cdot [7], [10] \\ (2, 11) \cdot \cdot \cdot [6], [11] \end{array} \right. \end{array} \right. \end{array} \right.$$

Уравнение (A), корнями которого являются суммы (8, 1), (8, 3), согласно правилам п. 351, оказывается следующим:  $x^2 + x - 4 = 0$ ; его корни равны  $-\frac{1}{2} + \frac{1}{2}\sqrt{17} \approx 1,5615528128$  и  $-\frac{1}{2} - \frac{1}{2}\sqrt{17} \approx -2,5615528128$ ; первый из них мы положим равным (8, 1), тогда второй обязательно равен (8, 3).

Далее, в качестве уравнения, корнями которого являются суммы (4, 1) и (4, 9), получается следующее уравнение (B):  $x^2 - (8, 1)x - 1 = 0$ ; корни его суть  $\frac{1}{2}(8, 1) \pm \frac{1}{2}\sqrt{4 + (8, 1)^2} \approx \frac{1}{2}(8, 1) \pm \frac{1}{2}\sqrt{12 + 3(8, 1) + 4(8, 3)}$ ; тот корень, у которого перед радикалом стоит положительный знак и который  $\approx 2,0494811777$ , мы примем за (4, 1), после чего другой корень, у которого величина радикала взята отрицательной, и численное значение которого

$\approx -0,4879283649$ , автоматически должен быть положен равным  $(4, 9)$ . Остальные суммы из четырех членов, именно,  $(4, 3)$  и  $(4, 10)$ , могут быть определены двояким способом. А именно, во-первых, — по методу п. 346, который дает следующие формулы, где для краткости вместо  $(4, 1)$  пишется  $p$ :

$$(4, 3) = -\frac{3}{2} + 3p - \frac{1}{2} p^3 \approx 0,3441507314,$$

$$(4, 10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2} p^3 \approx -2,9057035442.$$

Этот же метод приводит также к формуле  $(4, 9) = -1 - 6p + p^2 + p^3$ , из которой мы находим то же самое значение, которое мы только что привели. Во-вторых, суммы  $(4, 3)$ ,  $(4, 10)$  можно также определить посредством решения уравнения, корнями которого они являются. Это уравнение есть  $x^2 - (8, 3)x - 1 = 0$ , поэтому его корни суть  $\frac{1}{2}(8, 3) \pm \frac{1}{2}\sqrt{4 + (8, 3)^2}$ , т. е.  $\frac{1}{2}(8, 3) + \frac{1}{2}\sqrt{12 + 4(8, 1) + 3(8, 3)}$  и  $\frac{1}{2}(8, 3) - \frac{1}{2}\sqrt{12 + 4(8, 1) + 3(8, 3)}$ . А неопределенность, какой именно из этих корней есть  $(4, 3)$ , а какой есть  $(4, 10)$ , устраняется при помощи следующего приема, о котором мы и упоминали в п. 352. Преобразуем произведение  $(4, 1) - (4, 9)$  на  $(4, 3) - (4, 10)$ , в результате чего получим  $2(8, 1) - 2(8, 3)^*$ ; значение этого выражения, очевидно, положительно, а именно, равно  $+2\sqrt{17}$ , и, кроме того, первый сомножитель произведения тоже положителен, а именно, равен  $+\sqrt{12 + 3(8, 1) + 4(8, 3)}$ ; поэтому и второй сомножитель  $(4, 3) - (4, 10)$  должен обязательно быть положительным, и потому  $(4, 3)$  следует положить равным первому корню, у которого квадратный радикал берется со знаком  $+$ , а  $(4, 10)$  — второму корню. При этом, конечно, получаются те же самые численные значения, что и выше.

---

\* Истинная природа этого выражения такова, что это произведение в развернутом виде не содержит сумм по четыре члена, а выражается только через суммы из восьми членов; причина этого, на которой мы здесь ради краткости не останавливаемся, должна быть ясна для понимающего читателя.

После того как все суммы из четырех членов найдены, мы переходим к определению сумм из двух членов. В качестве уравнения (C), корнями которого являются содержащиеся в (4, 1) суммы (2, 1) и (2, 13), мы получаем  $x^2 - (4, 1)x + (4, 3) = 0$ ; его корни суть  $\frac{1}{2}(4, 1) \pm \frac{1}{2}\sqrt{-4(4, 3) + (4, 1)^2}$ , или  $\frac{1}{2}(4, 1) \pm \frac{1}{2}\sqrt{4 + (4, 9) - 2(4, 3)}$ . Тот корень, у которого величина радикала принимается положительной, и который приближенно равен 1,8649444588, мы полагаем равным (2, 1), так что другой корень, приближенно равный 0,1845367189, есть (2, 13). Если остальные суммы из двух членов мы захотим получить по методу п. 346, то для (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8) можно применить те же формулы, которые мы указали в предыдущем примере для точно так же обозначенных величин, именно,  $(2, 2)$  [или  $(2, 15)$ ]  $= (2, 1)^2 - 2$ , и т. д. Если же мы предпочтем получать эти суммы попарно решением квадратных уравнений, то для (2, 9) и (2, 15) мы найдем уравнение  $x^2 - (4, 9)x + (4, 10) = 0$ , корни которого суть  $\frac{1}{2}(4, 9) \pm \sqrt{4 + (4, 1) - 2(4, 10)}$ ; а то, как здесь разобратся в вопросе с двойным знаком, решается точно так же, как выше. Именно, при преобразовании произведения  $(2, 1) - (2, 13)$  на  $(2, 9) - (2, 15)$  получается  $-(4, 1) + (4, 9)$ , и так как это выражение, очевидно, отрицательно, а сомножитель  $(2, 1) - (2, 13)$  положителен, то  $(2, 9) - (2, 15)$  обязательно должно быть отрицательно, и потому в указанном перед этим выражении верхний знак должен быть взят для (2, 15), а нижний — для (2, 9). Отсюда мы находим, что  $(2, 9) = -1,9659461994$ ,  $(2, 15) = 1,4780178344$ . Точно так же мы заключаем (так как произведение  $(2, 1) - (2, 13)$  на  $(2, 3) - (2, 5)$  равно  $(4, 9) - (4, 10)$ , т. е. равно положительной величине), что сомножитель  $(2, 3) - (2, 5)$  положителен. После этого таким же вычислением, как и раньше, мы находим:

$$(2, 3) = \frac{1}{2}(4, 3) + \frac{1}{2}\sqrt{4 + (4, 10) - 2(4, 9)} \approx 0,8914767116,$$

$$(2, 5) = \frac{1}{2}(4, 3) - \frac{1}{2}\sqrt{4 + (4, 10) - 2(4, 9)} \approx -0,5473259801.$$

Наконец, посредством совершенно аналогичных операций находим

$$(2, 10) = \frac{1}{2} (4, 10) - \frac{1}{2} \sqrt{4 + (4, 3) - 2(4, 1)} \approx -1,7004342715,$$

$$(2, 11) = \frac{1}{2} (4, 10) + \frac{1}{2} \sqrt{4 + (4, 3) - 2(4, 1)} \approx -1,2052692728.$$

Теперь мы должны только дойти до самих корней из  $\Omega$ . В качестве уравнения  $(D)$ , корнями которого являются [1] и [16], мы получаем  $x^2 - (2, 1)x + 1 = 0$ , поэтому корни равны  $\frac{1}{2} (2, 1) \pm \frac{1}{2} \sqrt{(2, 1)^2 - 4}$ , т. е.  $\frac{1}{2} (2, 1) \pm \frac{1}{2} i \sqrt{4 - (2, 1)^2}$ , или  $\frac{1}{2} (2, 1) \pm \frac{1}{2} i \sqrt{2 - (2, 15)}$ . Верхний знак мы выбираем для [1], нижний — для [16]. Четырнадцать остальных корней мы получаем либо возведением в степени корня [1], либо решением семи квадратных уравнений, каждое из которых дает по два корня, причем неопределенность относительно знаков квадратных корней устраняется при помощи того же приема, что и ранее. Так, например, [4] и [13] являются корнями уравнения  $x^2 - (2, 13)x + 1 = 0$ , и потому равны  $\frac{1}{2} (2, 13) \pm \frac{1}{2} i \sqrt{2 - (2, 9)}$ . Но произведение [1] — [16] на [4] — [13] равно  $(2, 5) - (2, 3)$ , т. е. является вещественной отрицательной величиной; а так как [1] — [16] =  $i \sqrt{2 - (2, 15)}$ , т. е. есть произведение мнимой величины  $i$  на *положительную* вещественную величину, то, в силу  $i^2 = -1$ , [4] — [13] также должно быть произведением  $i$  на некоторую *положительную* вещественную величину. Отсюда мы заключаем, что для [4] нужно взять верхний, а для [13] нижний знак. Аналогичным образом для корней [8] и [9] мы находим значения  $\frac{1}{2} (2, 9) \pm \frac{1}{2} i \sqrt{2 - (2, 1)}$ , причем так как произведение [1] — [16] на [8] — [9] равно  $(2, 9) - (2, 10)$ , т. е. отрицательно, то для [8] нужно взять верхний, а для [9] нижний знак. Если таким же образом вычислить остальные корни, то получатся следующие численные значения, где верхний знак нужно брать для первого корня, а нижний для второго:

$$\begin{aligned}
[1], [16] &\approx 0,9324722294 \pm 0,3612416662 i, \\
[2], [15] &\approx 0,7390089172 \pm 0,6736956436 i, \\
[3], [14] &\approx 0,4457383558 \pm 0,8951632914 i, \\
[4], [13] &\approx 0,0922683595 \pm 0,9957341763 i, \\
[5], [12] &\approx -0,2736629901 \pm 0,9618256432 i, \\
[6], [11] &\approx -0,6026346364 \pm 0,7980172273 i, \\
[7], [10] &\approx -0,8502171357 \pm 0,5264321629 i, \\
[8], [9] &\approx -0,9829730997 \pm 0,1837495178 i.
\end{aligned}$$

Изложенного до сих пор вполне достаточно для решения уравнения  $x^n - 1 = 0$  и потому также и для нахождения тригонометрических функций, соответствующих дугам, сравнимым с полной окружностью; однако вследствие важности этого вопроса мы не можем закончить это исследование без того, чтобы не добавить кое-что из этой сокровищницы, относящееся как к самому этому вопросу, так и к связанным с ним задачам. При этом мы выберем отсюда то, что может быть изложено без введения нового громоздкого аппарата, и будем рассматривать это только как начатки этой обширной теории, которую в дальнейшем необходимо подробно разработать.

**Дальнейшие исследования о периодах корней.**

**Суммы, у которых количество членов четно,  
являются вещественными величинами**

### 355

Так как  $n$  всегда предполагается нечетным, то 2 находится среди сомножителей числа  $n - 1$ , и совокупность  $\Omega$  состоит из  $(n - 1)/2$  периодов по два члена. Период вида  $(2, \lambda)$  будет состоять из  $[\lambda]$  и  $[\lambda g^{(n-1)/2}]$ , где  $g$ , как и выше, обозначает некоторый первообразный корень по модулю  $n$ . Но  $g^{(n-1)/2} \equiv -1 \pmod{n}$ , и потому  $\lambda g^{(n-1)/2} \equiv -\lambda \pmod{n}$  (ср. п. 62), откуда  $[\lambda g^{(n-1)/2}] = [-\lambda]$ . Следовательно, если положить  $[\lambda] = \cos \frac{kP}{n} + i \sin \frac{kP}{n}$  и потому  $[-\lambda] = \cos \frac{kP}{n} - i \sin \frac{kP}{n}$ , то  $(2, \lambda) = 2 \cos \frac{kP}{n}$ . Из этого мы пока сделаем только

тот вывод, что значение каждой суммы из двух членов есть вещественная величина. Так как каждый период, число членов которого четно и равно  $2a$ , может быть разложен на  $a$  периодов по два члена, то значение каждой суммы четного числа членов всегда вещественно. Таким образом, если в п. 352 мы в ряду сомножителей  $\alpha, \beta, \gamma, \dots$  на последнем месте поместим число 2, то все операции, используемые вплоть до получения двучленных сумм, будут приводить к вещественным числам и мнимые величины смогут появиться только при переходе от двучленных сумм к самим корням.

### Об уравнении, определяющем разбиение корней из $\Omega$ на два периода

356

Большого внимания заслуживают вспомогательные уравнения, посредством которых для каждого значения  $n$  определяются суммы, образующие совокупность  $\Omega$ ; эти уравнения оказываются замечательным образом связанными с самыми глубоко скрытыми свойствами числа  $n$ . Однако в этом месте мы ограничим наше исследование только следующими двумя случаями. Сначала мы рассмотрим *квадратное уравнение, корнями которого являются суммы из  $(n-1)/2$  членов*, а затем, в случае, когда  $n-1$  делится на 3, — *кубическое уравнение, корни которого суть суммы из  $\frac{1}{3}(n-1)$  членов*.

Если мы ради краткости вместо  $\frac{1}{2}(n-1)$  будем писать  $m$ , и обозначим через  $g$  некоторый первообразный корень по модулю  $n$ , то совокупность  $\Omega$  будет состоять из двух периодов  $(m, 1)$  и  $(m, g)$ , причем первый будет содержать корни  $[1], [g^2], [g^4], \dots, [g^{n-3}]$ , а второй — корни  $[g], [g^3], [g^5], \dots, [g^{n-2}]$ . Если обозначить наименьшие положительные вычеты чисел  $g^2, g^4, \dots, g^{n-3}$  (безразлично в каком порядке) через  $R, R', R'', \dots$ , а наименьшие положительные вычеты чисел  $g, g^3, \dots, g^{n-2}$  (тоже в произвольном порядке) через  $N, N', N'', \dots$ , то корни, из которых состоит  $(m, 1)$ , будут совпадать с  $[1], [R], [R'], [R''], \dots$ , а корни из  $(m, g)$  — с  $[N], [N'], [N''], \dots$ . Но ясно, что все числа  $1, R, R', R'', \dots$  являются квад-



ратичными вычетами по модулю  $n$ , и так как все они меньше чем  $n$  и притом различны, так что количество их равно  $\frac{1}{2}(n-1)$ , т. е. равно количеству всех положительных вычетов по модулю  $n$ , меньших чем  $n$ , то эти числа полностью совпадают с указанной совокупностью вычетов. Отсюда сразу вытекает, что числа  $N, N', N'', \dots$ , которые различны как между собой, так и отличны от всех чисел  $1, R, R', R'', \dots$  и вместе с последними исчерпывают всю совокупность  $1, 2, 3, \dots, n-1$ , обязаны совпадать со всеми положительными квадратичными невычетами по модулю  $n$ , меньшими чем  $n$ . Если мы теперь предположим, что уравнение, корнями которого являются суммы  $(m, 1), (m, g)$ , есть

$$x^2 - Ax + B = 0,$$

то

$$A = (m, 1) + (m, g) = -1, \quad B = (m, 1) \cdot (m, g).$$

Произведение  $(m, 1)$  на  $(m, g)$ , согласно п. 345, равно

$$(m, N+1) + (m, N'+1) + (m, N''+1) + \dots = W,$$

и может быть представлено в виде  $\alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$ . Для определения коэффициентов  $\alpha, \beta, \gamma$  мы заметим, во-первых, что  $\alpha + \beta + \gamma = m$  (в силу того, что количество сумм в  $W$  равно  $m$ ), во-вторых, что  $\beta = \gamma$  (это следует из п. 350, ибо произведение  $(m, 1) \cdot (m, g)$  является симметрической функцией сумм  $(m, 1), (m, g)$ , из которых состоит большая сумма  $(n-1, 1)$ ); в-третьих, так как все числа  $N+1, N'+1, N''+1, \dots$  заключены в границах между 2 и  $n+1$  (исключая самые границы), то ясно, что либо ни одна из сумм из  $W$  не сводится к  $(m, 0)$  (и потому  $\alpha = 0$ ), что будет в том случае, когда среди чисел  $N, N', N'', \dots$  число  $n-1$  не содержится, либо к  $(m, 0)$  сводится только одна сумма, а именно,  $(m, n)$ , что будет в том случае, когда  $n-1$  находится среди чисел  $N, N', N'', \dots$ , и тогда  $\alpha = 1$ . Из этого мы заключаем, что в первом случае  $\alpha = 0, \beta = \gamma = \frac{1}{2}m$ , а во втором случае  $\alpha = 1, \beta = \gamma = \frac{1}{2}(m-1)$ ; одновременно отсюда следует, так как числа  $\beta$  и  $\gamma$  обязательно целые, что имеет место первый случай (или, что то же

самое, что  $n - 1$  или  $-1$  не содержится среди невычетов по модулю  $n$ ), если  $m$  четно, т. е.  $n$  имеет вид  $4k + 1$ ; второй же случай имеет место (это равносильно тому, что  $n - 1$  или  $-1$  содержится среди невычетов по модулю  $n$ ), если  $m$  нечетно, т. е.  $n$  имеет вид  $4k + 3$  \*. Следовательно, так как  $(m, 0) = m$  и  $(m, 1) + \dots + (m, g) = -1$ , искомое произведение в первом случае равно  $-\frac{1}{2}m$ , а во втором случае равно  $\frac{1}{2}(m + 1)$ , а потому искомым уравнением в первом случае является  $x^2 + x - \frac{1}{4}(n - 1) = 0$  (корни  $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$ ), а во втором будет  $x^2 + x + \frac{1}{4}(n + 1) = 0$  (корни  $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$ ).

Таким образом, какой бы корень из  $\Omega$  ни был взят в качестве [1], разность между суммами  $\sum [\mathfrak{K}]$  и  $\sum [\mathfrak{N}]$ , где в качестве  $\mathfrak{K}$  нужно подставить все положительные вычеты, а в качестве  $\mathfrak{N}$  — все положительные невычеты по модулю  $n$ , меньшие чем  $n$ , равна  $\pm\sqrt{n}$  для  $n \equiv 1 \pmod{4}$  и равна  $\pm i\sqrt{n}$  для  $n \equiv 3 \pmod{4}$ . Отсюда легко видеть также, что если  $k$  обозначает целое число, не делящееся на  $n$ , то

$$\sum \cos \frac{k\mathfrak{K}P}{n} - \sum \cos \frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \text{ и } \sum \sin \frac{k\mathfrak{K}P}{n} - \sum \sin \frac{k\mathfrak{N}P}{n} = 0$$

для  $n \equiv 1 \pmod{4}$ , а для  $n \equiv 3 \pmod{4}$  первая разность равна 0, а вторая равна  $\pm\sqrt{n}$ ; эти теоремы исключительно изящны. Заметим также, что всегда нужно брать верхний знак, если  $k$  равно 1, или, более общо, равно некоторому квадратичному вычету по модулю  $n$ , и нижний знак, если  $k$  есть квадратичный невычет по модулю  $n$ . Теоремы эти не только без ущерба, но скорее с выигрышем в изя-

---

\* Таким образом, мы получили новое доказательство теоремы о том, что  $-1$  является вычетом по всем простым числам вида  $4k + 1$  и невычетом по всем простым числам вида  $4k + 3$ , которая выше (пп. 108, 109, 262) уже была доказана многими различными способами. Если бы мы захотели здесь предполагать эту теорему известной, то было бы не нужно обращать внимание на различие двух случаев в этом условии, так как  $\beta, \gamma$  сами по себе уже были бы целыми числами.

щества могут быть распространены и на составные значения  $n$ ; однако этого вопроса, требующего более глубоких исследований, мы здесь не будем касаться, а отложим это до другого случая.

### Доказательство теоремы, упомянутой в разделе IV

357

Если уравнение, корнями которого являются  $m$  содержащихся в периоде  $(m, 1)$  корней, есть

$$z = x^m - ax^{m-1} + bx^{m-2} - \dots = 0,$$

то  $a = (m, 1)$ , и остальные коэффициенты  $b, \dots$  имеют вид  $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ , где  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$  суть целые числа (п. 348); если при этом обозначить через  $z'$  функцию, в которую переходит  $z$ , если вместо  $(m, 1)$  всюду подставить  $(m, g)$ , и вместо  $(m, g)$  подставить  $(m, g^2)$  или, что то же самое,  $(m, 1)$ , то корнями уравнения  $z' = 0$  будут корни, содержащиеся в  $(m, g)$ , и будет иметь место

$$zz' = \frac{x^n - 1}{x - 1} = X.$$

Поэтому  $z$  может быть представлено в виде  $R + S(m, 1) + T(m, g)$ , где  $R, S, T$  являются целыми функциями от  $x$ , все коэффициенты которых в свою очередь являются целыми числами. После этого мы будем иметь

$$z' = R + S(m, g) + T(m, 1).$$

Отсюда следует, если ради краткости обозначить через  $p$  и  $q$  соответственно  $(m, 1)$  и  $(m, g)$ , что

$$\begin{aligned} 2z &= 2R + (S + T)(p + q) - (T - S)(p - q) = \\ &= 2R - S - T = -(T - S)(p - q), \end{aligned}$$

и аналогично

$$2z' = 2R - S - T + (T - S)(p - q).$$

Поэтому, если мы положим

$$2R - S - T = Y, \quad T - S = Z,$$

то  $4X = Y^2 - (p - q)^2 Z^2$ , и потому, в силу  $(p - q)^2 = \pm n$ ,

$$4X = Y^2 \mp nZ^2,$$

причем нужно брать верхний знак, если  $n$  имеет вид  $4k + 1$ , и нижний, если  $n$  имеет вид  $4k + 3$ . Это и есть теорема, доказательство которой мы выше (п. 124) обещали привести. Легко видеть, что два старших члена функции  $Y$  всегда суть  $2x^m + x^{m-1}$ , а старший член функции  $Z$  всегда есть  $x^{m-1}$ ; остальные коэффициенты, которые все, очевидно, являются целыми числами, зависят от различных свойств числа  $n$  и не могут быть охвачены общими аналитическими формулами.

**Пример.** Для  $n = 17$  в качестве уравнения, корнями которого являются восемь корней, содержащихся в  $(8, 1)$ , мы, согласно правилам п. 348, находим уравнение

$$x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 - \\ - (4p + 3q)x^3 + (4 + p + 2q)x^2 - px + 1 = 0,$$

откуда получается, что

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1,$$

$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x,$$

$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2,$$

и потому

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2,$$

$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + 2.$$

Ниже приводится еще несколько других примеров.

| $n$ | $Y$                                                                                          | $Z$                                                          |
|-----|----------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 3   | $2x + 1$                                                                                     | 1                                                            |
| 5   | $2x^2 + x + 2$                                                                               | $x$                                                          |
| 7   | $2x^3 + x^2 - x - 2$                                                                         | $x^2 + x$                                                    |
| 11  | $2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$                                                           | $x^4 + x$                                                    |
| 13  | $2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2$                                                     | $x^5 + x^3 + x$                                              |
| 19  | $2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - \\ - 5x^4 - 3x^3 + 4x^2 - x - 2$                          | $x^8 - x^6 + x^5 + x^4 - \\ - x^3 + x$                       |
| 23  | $2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - \\ - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5x^2 - \\ - x - 2$ | $x^{10} + x^9 - x^7 - \\ - 2x^6 - 2x^5 - x^4 + x^2 + \\ + x$ |

## Об уравнении для разбиения корней из $\Omega$ на три периода

358

Мы переходим к рассмотрению кубических уравнений, при помощи которых в случае, когда  $n$  имеет вид  $3k + 1$ , определяются три суммы из  $\frac{1}{3}(n - 1)$  членов, образующие совокупность  $\Omega$ . Пусть  $g$  — некоторый первообразный корень по модулю  $n$  и  $\frac{1}{3}(n - 1) = m$  ( $m$  есть целое четное число). Тогда тремя суммами, из которых состоит  $\Omega$ , будут  $(m, 1)$ ,  $(m, g)$ ,  $(m, g^2)$ , которые мы обозначим через  $p$ ,  $p'$ ,  $p''$ , и ясно, что первая содержит корни  $[1]$ ,  $[g^3]$ ,  $[g^6]$ ,  $\dots$ ,  $[g^{n-4}]$ , вторая — корни  $[g]$ ,  $[g^4]$ ,  $\dots$ ,  $[g^{n-3}]$ , третья — корни  $[g^2]$ ,  $[g^5]$ ,  $\dots$ ,  $[g^{n-2}]$ . Если предположить, что искомое уравнение есть

$$x^3 - Ax^2 + Bx - C = 0,$$

то

$$A = p + p' + p'', \quad B = pp' + p'p'' + pp'', \quad C = pp'p'',$$

откуда тотчас же получается  $A = -1$ . Пусть наименьшие положительные вычеты чисел  $g^3, g^6, \dots, g^{n-4}$  по модулю  $n$  суть (в произвольном порядке)  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$ , и  $\mathfrak{K}$  — их совокупность с присоединением к ней числа 1; точно так же пусть  $\mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \dots$  — наименьшие положительные вычеты чисел  $g, g^4, g^7, \dots, g^{n-3}$ , и  $\mathfrak{K}'$  — их совокупность; наконец, пусть  $\mathfrak{A}'', \mathfrak{B}'', \mathfrak{C}'', \dots$  — наименьшие положительные вычеты чисел  $g^2, g^5, g^8, \dots, g^{n-2}$ , и  $\mathfrak{K}''$  — их совокупность; тогда все числа из  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$  будут различны и вместе охватывают числа  $1, 2, 3, \dots, n - 1$ . Прежде всего нужно заметить, что число  $n - 1$  обязательно находится в  $\mathfrak{K}$ , так как легко видеть, что оно является вычетом числа  $g^{3m/2}$ . Отсюда легко видеть также, что пара чисел типа  $h$  и  $n - h$  должна содержаться в одной и той же из трех совокупностей  $\mathfrak{K}, \mathfrak{K}', \mathfrak{K}''$ , так как если первое является вычетом числа  $g^\lambda$ , то другое будет вычетом числа  $g^{\lambda + \frac{3m}{2}}$  или числа  $g^{\lambda - \frac{3m}{2}}$ , если  $\lambda > \frac{3m}{2}$ . Обозначим через  $(\mathfrak{K}\mathfrak{K})$  коли-

чество таких чисел из ряда  $1, 2, 3, \dots, n-1$ , что и они сами и числа, получающиеся из них прибавлением единицы, содержатся в  $\mathfrak{K}$ , через  $(\mathfrak{K}\mathfrak{K}')$  — количество чисел этого же ряда, которые сами содержатся в  $\mathfrak{K}$ , но непосредственно следующие за ними числа содержатся в  $\mathfrak{K}'$ ; аналогичный смысл имеют и обозначения  $(\mathfrak{K}\mathfrak{K}'')$ ,  $(\mathfrak{K}'\mathfrak{K})$ ,  $(\mathfrak{K}'\mathfrak{K}')$ ,  $(\mathfrak{K}'\mathfrak{K}'')$ ,  $(\mathfrak{K}''\mathfrak{K})$ ,  $(\mathfrak{K}''\mathfrak{K}')$ ,  $(\mathfrak{K}''\mathfrak{K}'')$ . Теперь мы утверждаем, *во-первых*, что  $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$ . Действительно, если мы предположим, что  $h, h', h'', \dots$  суть всевозможные числа из ряда  $1, 2, 3, \dots, n-1$ , которые сами содержатся в  $\mathfrak{K}$ , в то время как следующие за ними числа  $h+1, h'+1, h''+1, \dots$  содержатся в  $\mathfrak{K}'$ , и число которых, следовательно, равно  $(\mathfrak{K}\mathfrak{K}')$ , то ясно, что все числа  $n-h-1, n-h'-1, n-h''-1, \dots$  содержатся в  $\mathfrak{K}'$ , следующие за ними числа  $n-h, n-h', \dots$  — в  $\mathfrak{K}$ ; а так как подобных чисел всего имеется  $(\mathfrak{K}'\mathfrak{K})$ , то не может быть  $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$ , и точно так же доказывается, что не может быть и  $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$ ; поэтому оба числа обязательно должны быть равны. Совершенно таким же образом доказывается, что  $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$ ,  $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$ . *Во-вторых*, так как каждое число из  $\mathfrak{K}$ , за исключением только одного наибольшего числа  $n-1$ , имеет следующее за ним, которое содержится либо в  $\mathfrak{K}$ , либо в  $\mathfrak{K}'$ , либо в  $\mathfrak{K}''$ , то сумма  $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$  равна уменьшенному на единицу количеству всех чисел, т. е. равна  $m-1$ , и по аналогичной причине

$$(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m.$$

После этих приготовлений мы представим, в соответствии с п. 345, произведение  $pp'$  в виде  $(m, \mathfrak{A}' + 1) + (m, \mathfrak{B}' + 1) + \dots$ ; это выражение, как легко видеть, равно  $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$  и так как, согласно п. 345, I, произведение  $p'p''$  получается из  $pp'$ , если вместо  $(m, 1)$ ,  $(m, g)$ ,  $(m, g^2)$  подставить соответственно  $(m, g)$ ,  $(m, g^2)$ ,  $(m, g^3)$ , т. е. вместо  $p, p', p''$  подставить  $p', p'', p$ , то  $p'p'' = (\mathfrak{K}'\mathfrak{K})p' + (\mathfrak{K}'\mathfrak{K}')p'' + (\mathfrak{K}'\mathfrak{K}'')p$ , и совершенно аналогично,  $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$ . Отсюда тотчас же следует, что, *во-первых*,

$$B = m(p + p' + p'') = -m,$$

и *во-вторых*, так как подобно тому, как было представлено  $pp'$ ,

можно и  $pp''$  записать в виде  $(\mathfrak{R}''\mathfrak{R})p + (\mathfrak{R}''\mathfrak{R}')p' + (\mathfrak{R}''\mathfrak{R}'')p''$ , а это выражение должно быть равно тому, которое было указано для  $pp''$  выше, то обязательно  $(\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}'\mathfrak{R}')$  и  $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R})$ . Если теперь положить

$(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a$ ,  $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}') = b$ ,  $(\mathfrak{R}'\mathfrak{R}') = (\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}'') = c$ , то из сказанного следует, что  $m - 1 = (\mathfrak{R}\mathfrak{R}) + (\mathfrak{R}\mathfrak{R}') + (\mathfrak{R}\mathfrak{R}'') = (\mathfrak{R}\mathfrak{R}) + b + c$ , и  $a + b + c = m$ , т. е.  $(\mathfrak{R}\mathfrak{R}) = a - 1$ , так что наши девять неизвестных величин сводятся к трем, именно, к  $a$ ,  $b$ ,  $c$ , а в силу равенства  $a + b + c = m$  даже к двум. Наконец, квадрат числа  $p$ , очевидно, представляется в виде  $(m, 1 + 1) + (m, \mathfrak{A} + 1) + \dots$ ; среди слагаемых этого выражения имеется  $(m, n)$ , которое равно  $(m, 0)$ , т. е. равно  $m$ , в то время как остальные слагаемые, как легко видеть, сводятся к  $(\mathfrak{R}\mathfrak{R})p + (\mathfrak{R}\mathfrak{R}')p' + (\mathfrak{R}\mathfrak{R}'')p''$ ; поэтому мы имеем  $p^2 = m + (a - 1)p + bp' + cp''$ .

Таким образом, мы, согласно предыдущим исследованиям, имеем следующие четыре равенства:

$$\begin{aligned} p^2 &= m + (a - 1)p + bp' + cp'', \\ pp' &= bp + cp' + ap'', \\ pp'' &= cp + ap' + bp'', \\ p'p'' &= ap + bp' + cp'', \end{aligned}$$

где три неизвестных величины  $a$ ,  $b$ ,  $c$  связаны соотношением

$$(I) \quad a + b + c = m,$$

и, кроме того, заведомо являются целыми числами. Отсюда следует, что

$$\begin{aligned} C = pp'p'' &= ap^2 + bpp' + cpp'' = \\ &= am + (a^2 + b^2 + c^2 - a)p + (ab + ac + bc)p' + (ab + bc + ac)p''. \end{aligned}$$

Но так как  $pp'p''$  является симметрической функцией сумм  $p$ ,  $p'$ ,  $p''$ , то коэффициенты, на которые эти суммы умножаются в предыдущем выражении, обязательно должны быть равны, вследствие чего мы получаем новое уравнение

$$(II) \quad a^2 + b^2 + c^2 - a = ab + bc + ac,$$

откуда следует, что  $C = at + (ab + bc + ca)(p + p' + p'')$ , или (в силу того, что  $p + p' + p'' = -1$  и на основании (I))  
(III)  $C = a^2 - bc.$

Хотя теперь  $C$  зависит от трех неизвестных, между которыми мы имеем только два соотношения, тем не менее этого оказывается достаточным для окончательного определения  $C$ , если только использовать еще то условие, что  $a, b, c$  являются целыми числами. Чтобы показать это, представим уравнение (II) в виде

$$12a + 12b + 12c + 4 = \\ = 36a^2 + 36b^2 + 36c^2 - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4.$$

Левая часть, согласно (I), равна  $12m + 4 = 4n$ , а правая — преобразуется в

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2,$$

или, если вместо  $2a - b - c$  написать  $k$ , в  $(3k - 2)^2 + 27(b - c)^2$ . Из этого вытекает, что число  $4n$  (т. е. вообще четвертая кратность каждого простого числа вида  $3m + 1$ ) может быть представлено формой  $x^2 + 27y^2$ , результат, который, впрочем, легко может быть выведен из теории двойничных форм; все же представляется замечательным, что такое разложение связано со значениями  $a, b, c$ . Но число  $4n$  только одним способом может быть разложено на сумму квадрата и двадцать седьмой кратности квадрата, что мы докажем следующим образом\*. Пусть

$$4n = t^2 + 27u^2 = t'^2 + 27u'^2;$$

тогда, во-первых,

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16n^2,$$

во-вторых,

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16n^2,$$

в-третьих,

$$(tu' + t'u)(tu' - t'u) = 4n(u'^2 - u^2);$$

из третьего равенства следует, так как  $n$  простое число, что оно входит в одно из чисел  $tu' + t'u$ ,  $tu' - t'u$ ; но из первого и вто-

---

\* Более прямым методом эту теорему можно было бы доказать на основании принципов пятого раздела.



рого равенств вытекает, что оба эти числа меньше чем  $n$ ; поэтому то из них, которое делится на  $n$ , обязательно равно 0, следовательно  $u'^2 - u^2 = 0$ , откуда  $u'^2 = u^2$  и  $t'^2 = t^2$ , т. е. оба разложения не являются различными. Поэтому, если предполагать известным разложение числа  $4n$  на квадрат и двадцать седьмую кратность квадрата (это разложение можно получить либо данным в пятом разделе прямым методом, либо изложенным в пп. 323, 324 косвенным методом), именно, предположить, что  $4n = M^2 + 27N^2$ , то определятся квадраты  $(3k - 2)^2$ ,  $(b - c)^2$ , и вместо уравнения (II) мы получаем теперь два уравнения. Но легко видеть, что не только квадрат  $(3k - 2)^2$ , но и само число  $3k - 2$  полностью определено; действительно, так как оно обязательно равно либо  $+M$  либо  $-M$ , то неопределенность знака устраняется условием, что  $k$  должно быть целым числом. Именно, нужно положить  $3k - 2 = +M$ , или  $-M$  в зависимости от того, имеет ли  $M$  вид  $3z + 1$  или  $3z + 2$  \*. Так как теперь  $k = 2a - b - c = 3a - m$ , то  $a = \frac{1}{3}(m + k)$ ,  $b + c = m - a = \frac{1}{3}(2m - k)$ , и потому

$$\begin{aligned} C &= a^2 - bc = a^2 - \frac{1}{4}(b + c)^2 + \frac{1}{4}(b - c)^2 = \\ &= \frac{1}{9}(m + k)^2 - \frac{1}{36}(2m - k)^2 + \frac{1}{4}N^2 = \frac{1}{12}k^2 + \frac{1}{3}km + \frac{1}{4}N^2, \end{aligned}$$

и таким же способом находятся все коэффициенты. Эта формула станет еще проще, если вместо  $N^2$  подставить его значение из уравнения  $(3k - 2)^2 + 27N^2 = 4n = 12m + 4$ ; после соответствующих вычислений получается

$$C = \frac{1}{9}(m + k + 3km) = \frac{1}{9}(m + kn).$$

---

\* Очевидно, что  $M$  не может иметь вид  $3z$ , так как тогда  $4n$  делилось бы на 3. На ту неопределенность, имеет ли место  $b - c = N$  или  $= -N$ , нам дальше не нужно будет обращать внимания, и она не может быть устранена по самой природе вещей, так как все зависит от выбора первообразного корня  $g$ , так что для одних первообразных корней разность  $b - c$  положительна, а для других отрицательна.

Это же значение может быть представлено и в виде  $(3k - 2)N^2 + k^3 - 2k^2 + k - kt + t$ , который хотя и менее удобен для применения, но зато сразу показывает, что  $C$ , как это и должно быть, является целым числом.

**Пример.** Для  $n = 19$  будет  $4n = 49 + 27$ , поэтому  $3k - 2 = +7$ ,  $k = 3$ ,  $C = \frac{1}{9}(6 + 57) = 7$ , и искомое уравнение, как и раньше, есть  $x^3 + x^2 - 6x - 7 = 0$ . Подобным же образом для  $n = 7, 13, 31, 37, 43, 61, 67$  значение  $k$  соответственно равно  $1, -1, 2, -3, -2, 1, -1$ , и потому  $C = 1, -1, 8, -11, -8, 9, -5$ .

Хотя вопрос, решенный в этом пункте, является довольно запутанным, мы не захотели обойти его, отчасти ввиду изящества решения, а также и потому, что это дало возможность использовать различные искусственные приемы, которые с большой пользой могут быть применены и в других исследованиях\*.

### Сведение уравнений, из которых находятся корни $\Omega$ , к чистым уравнениям

359

Предыдущие исследования относились к отысканию вспомогательных уравнений; теперь мы изложим весьма выдающееся свойство, касающееся их решения. Как известно, все усилия крупнейших математиков найти общее решение уравнений, степень которых выше четвертой, или (выражаясь точнее) найти редукцию произвольных уравнений к чистым уравнениям, до сих пор были тщетны, и едва ли можно сомневаться в том, что эта проблема не просто превосходит силы современного анализа, но и вообще неразрешима. (Сравните с тем, что по этому поводу замечается в п. 9 сочинения

---

\* Следствие. Если  $\varepsilon$  есть корень уравнения  $x^3 - 1 = 0$ , то  $(p + \varepsilon p' + \varepsilon^2 p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$ . Если положить  $\frac{M}{\sqrt{4n}} = \cos \varphi$ ,  $\frac{N\sqrt{27}}{\sqrt{4n}} = \sin \varphi$ , то  $p = -\frac{1}{3} + \frac{2}{3} \cos \frac{1}{3} \varphi \sqrt{n}$ ,  $M \equiv +1 \pmod{3}$ ,  $1 \equiv M(1 \cdot 2 \cdot 3 \cdots m)^3 \pmod{n}$ . Если положить  $3x + 1 = y$ , то будет иметь место равенство  $y^3 - 3ny - Mn = 0$ .

«Новое доказательство одной арифметической теоремы».) Тем не менее очевидно, что существует бесчисленное множество смешанных уравнений любой степени, которые допускают такое сведение к чистым уравнениям, и мы надеемся, что математикам будет интересно, если мы покажем, что наши вспомогательные уравнения всегда относятся к такому типу. Однако, вследствие большого объема этого исследования, мы укажем здесь только основные моменты, необходимые для доказательства возможности редукции, а более подробное изложение отложим до другого времени. Сначала должны быть предпосланы некоторые общие замечания о корнях уравнения  $x^e - 1 = 0$ , охватывающие также и тот случай, когда  $e$  является составным числом.

I. Эти корни (как известно из элементарных книг) представляются в виде  $\cos \frac{kP}{e} + i \sin \frac{kP}{e}$ , где в качестве  $k$  нужно взять  $e$  чисел  $0, 1, 2, 3, \dots, e-1$  или каких-либо других, сравнимых с этими по модулю  $e$ . Один корень, получающийся при  $k=0$  или вообще при делящемся на  $e$  значении  $k$ , равен 1; всем остальным значениям  $k$  соответствуют корни, отличные от 1.

II. Так как  $\left(\cos \frac{kP}{e} + i \sin \frac{kP}{e}\right)^\lambda = \cos \frac{\lambda kP}{e} + i \sin \frac{\lambda kP}{e}$ , то ясно, что если  $R$  есть корень, соответствующий взаимно простому с  $e$  значению  $k$ , то в прогрессии  $R, R^2, R^3, \dots$  только  $e$ -й член впервые будет равен 1, а все предыдущие будут от 1 отличны. Из этого тотчас же следует, что все  $e$  величин  $1, R, R^2, R^3, \dots, R^{e-1}$  различны, а так как все они, очевидно, удовлетворяют уравнению  $x^e - 1 = 0$ , то они представляют собой все корни этого уравнения.

III. Наконец, при том же предположении для каждого целого не делящегося на  $e$  значения  $\lambda$  будет иметь место равенство

$$1 + R^\lambda + R^{2\lambda} + \dots + R^{\lambda(e-1)} = 0;$$

действительно, сумма, стоящая в левой части, очевидно, равна  $(1 - R^{\lambda e})/(1 - R^\lambda)$ , а числитель этой дроби равен 0, в то время как знаменатель отличен от 0. Если же  $\lambda$  делится на  $e$ , то указанная сумма, очевидно, равна  $e$ .

Пусть, как и всюду до этого,  $n$  есть простое число,  $g$  — первообразный корень по модулю  $n$ , и  $n - 1$  — произведение трех целых положительных чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ . Ради краткости мы сразу же поведем исследование так, чтобы оно распространялось и на случай, когда одно из чисел  $\alpha$  или  $\gamma$  равно 1; если  $\gamma = 1$ , то в качестве сумм  $(\gamma, 1)$ ,  $(\gamma, g)$ ,  $\dots$  надо взять корни  $[1]$ ,  $[g]$ ,  $\dots$ . Таким образом, из всех предполагающихся известными  $\alpha$  сумм по  $\beta\gamma$  членов,  $(\beta\gamma, 1)$ ,  $(\beta\gamma, g)$ ,  $(\beta\gamma, g^2)$ ,  $\dots$ ,  $(\beta\gamma, g^{\alpha} - 1)$ , нужно получить суммы по  $\gamma$  членов — задача, которую выше мы свели к решению уравнения степени  $\beta$ , но, как мы теперь покажем, которую можно решить и при помощи чистого уравнения такой же степени. Ради краткости мы обозначим суммы

$$(\gamma, 1), (\gamma, g^{\alpha}), (\gamma, g^{2\alpha}), \dots, (\gamma, g^{\alpha\beta - \alpha}),$$

содержащиеся в  $(\beta\gamma, 1)$ , соответственно через  $a, b, c, \dots, m$ ; суммы

$$(\gamma, g), (\gamma, g^{\alpha + 1}), (\gamma, g^{2\alpha + 1}), \dots, (\gamma, g^{\alpha\beta - \alpha + 1}),$$

содержащиеся в  $(\beta\gamma, g)$ , — соответственно через  $a', b', c', \dots, m'$ ; суммы

$$(\gamma, g^2), (\gamma, g^{\alpha + 2}), \dots, (\gamma, g^{\alpha\beta - \alpha + 2})$$

— соответственно через  $a'', b'', \dots, m''$ , и т. д., до тех сумм, которые содержатся в  $(\beta\gamma, g^{\alpha} - 1)$ .

I. Пусть теперь  $R$  обозначает любой корень уравнения  $x^{\beta} - 1 = 0$  и пусть выражение для  $\beta$ -й степени функции

$$t = a + Rb + R^2c + \dots + R^{\beta - 1}m,$$

найденное по правилам п. 345, имеет вид

$$\begin{aligned} N + Aa + Bb + Cc + \dots + Mm + A'a' + B'b' + C'c' + \dots + M'm' + \\ + A''a'' + B''b'' + C''c'' + \dots + M''m'' + \\ + \dots = T, \end{aligned}$$

где все коэффициенты  $N, A, B, A', \dots$  являются целыми рациональными функциями от  $R$ . Если предположить далее, что  $\beta$ -е степени двух других функций

$$u = R^{\beta}a + Rb + R^2c + \dots + R^{\beta - 1}m,$$

$$u' = b + Rc + R^2d + \dots + R^{\beta-2}m + R^{\beta-1}a$$

суть соответственно  $U$  и  $U'$ , то так как  $u'$  получается из  $t$  заменой сумм  $a, b, c, \dots, m$  соответственно на  $b, c, d, \dots, a$ , мы, на основании п.350, легко получим, что

$$\begin{aligned} U' = & N + Ab + Bc + Cd + \dots + Ma + \\ & + A'b' + B'c' + C'd' + \dots + M'a' + \\ & + A''b'' + B''c'' + C''d'' + \dots + M''a'' + \\ & + \dots \end{aligned}$$

Далее, так как  $u = Ru'$ , то, очевидно,  $U = R^{\beta}U'$ ; поэтому, вследствие того, что  $R^{\beta} = 1$ , соответствующие коэффициенты у  $U$  и  $U'$  одинаковы; наконец, легко видеть, что так как  $t$  и  $u$  отличаются только тем, что у  $t$  сумма  $a$  умножена на 1, а у  $u$  — на  $R^{\beta}$ , то все соответствующие коэффициенты (т. е. коэффициенты при одинаковых суммах) у  $T$  и  $U$  равны, а потому равны также и коэффициенты у  $T$  и  $U'$ . Отсюда следует, наконец, что  $A = B = C = \dots = M$ ,  $A' = B' = C' = \dots = M'$ ,  $A'' = B'' = C'' = \dots = M''$ , ..., так что  $T$  приводится к виду

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \dots,$$

где каждый из коэффициентов  $N, A, A', \dots$  имеет вид

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \dots,$$

причем  $p, p', p'', \dots$  являются заданными целыми числами.

II. Если в качестве  $R$  взять некоторый определенный корень уравнения  $x^{\beta} - 1 = 0$  (которое мы предполагаем уже решенным), причем такой, что никакая его степень, меньшая чем  $\beta$ -я, не равна 1, то  $T$  также будет определенной величиной, из которой  $t$  может быть получено решением чистого уравнения  $t^{\beta} - T = 0$ . Но так как это уравнение имеет  $\beta$  корней, которые равны  $t, Rt, R^2t, \dots, R^{\beta-1}t$ , то представляется неясным, какой именно корень нужно взять. Однако это совершенно безразлично, что можно пояснить следующим образом. Нужно вспомнить, что после того как все суммы из  $\beta\gamma$  членов определены, корень [1] определен лишь в том смысле, что так должен быть обозначен один из  $\beta\gamma$  корней, содержащихся в  $(\beta\gamma, 1)$ , и потому совершенно безразлично, какую из  $\beta$

сумм, образующих сумму  $(\beta\gamma, 1)$ , обозначить через  $a$ . Если теперь, после того как некоторая определенная сумма обозначена через  $a$ , предположить, что  $t = \mathfrak{Z}$ , то легко видеть, что если затем обозначить через  $a$  ту сумму, которая раньше была обозначена через  $b$ , то суммы, которые раньше обозначались через  $c, d, \dots, a, b$ , теперь будут  $b, c, \dots, m, a$ , и потому значение  $t$  теперь будет равно  $\frac{\mathfrak{Z}}{R} = \mathfrak{Z}R^{\beta-1}$ . Точно так же, если через  $a$  обозначить ту сумму, которая первоначально обозначалась через  $c$ , то значение  $t$  станет равным  $\mathfrak{Z}R^{\beta-2}$ , и вообще  $t$  можно рассматривать как равное любой из величин  $\mathfrak{Z}, \mathfrak{Z}R^{\beta-1}, \mathfrak{Z}R^{\beta-2}, \dots$ , т. е. любому корню уравнения  $x^{\beta} - T = 0$ , в зависимости от того, какая из содержащихся в  $(\beta\gamma, 1)$  сумм обозначена через  $(\gamma, 1)$ .

III. После того как величина  $t$  таким путем определена, нужно найти  $\beta - 1$  других равенств, которые получаются из  $t$ , если  $R$  заменять последовательно на  $R^2, R^3, R^4, \dots, R^{\beta}$ , именно,

$$\begin{aligned} t' &= a + R^2b + R^4c + \dots + R^{2\beta-2}m, \\ t'' &= a + R^3b + R^6c + \dots + R^{3\beta-3}m, \\ &\dots \dots \dots \end{aligned}$$

Последнее равенство мы, впрочем, уже знаем, так как оно, очевидно, есть  $a + b + c + \dots + m = (\beta\gamma, 1)$ ; остальные же могут быть получены следующим образом. Если мы точно так же, как в I было представлено  $t^{\beta}$ , представим, в соответствии с правилами п. 345, произведение  $t^{\beta-2}t'$ , то методом, совершенно аналогичным предыдущему, можно будет доказать, что результат можно будет представить в виде

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, g^2) + \dots = T',$$

где  $\mathfrak{N}, \mathfrak{A}, \mathfrak{A}', \dots$  являются целыми рациональными функциями от  $R$ , и потому  $T'$  будет известной величиной, из которой получается  $t' = \frac{T't^2}{T}$ . Если, далее, предположить, что для произведения  $t^{\beta-3}t''$  получается функция  $T''$ , то точно так же это выражение можно представить в аналогичной форме и получить затем значение  $t''$  в виде  $t'' = \frac{T''t^3}{T}$ ; точно так же  $t'''$  находится из равенства  $t''' = \frac{T'''t^4}{T}$ , где  $T'''$  есть известная величина, и т. д.

Этот метод был бы неприменим, если бы  $t$  могло равняться 0, откуда следовало бы тогда, что и  $T = T' = T'' = \dots = 0$ ; но можно показать, что это невозможно, хотя доказательство мы здесь опускаем, так как оно слишком длинно. Имеются также специальные приемы, при помощи которых дроби  $\frac{T'}{T}, \frac{T''}{T}, \dots$  преобразуются в целые рациональные функции от  $R$ , а также в случае  $\alpha = 1$  существуют более короткие методы для нахождения значений  $t', t'', \dots$ ; все это мы должны, однако, обойти здесь молчанием.

IV. Наконец, после того как  $t, t', t'', \dots$  найдены, мы, согласно замечанию III предыдущего пункта, имеем  $t + t' + t'' + \dots = \beta a$ , откуда определяется значение  $a$ , из которого, согласно п. 346, могут быть получены значения всех остальных сумм из  $\gamma$  членов. Значения  $b, c, d, \dots$  могут быть определены также из следующих равенств, справедливость которых должна быть ясна для каждого внимательного читателя:

$$\begin{aligned} \beta b &= R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \dots, \\ \beta c &= R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \dots, \\ \beta d &= R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \dots, \\ &\dots \end{aligned}$$

Из большого числа замечаний, которые можно сделать в отношении этого исследования, мы приведем здесь только одно. Что касается решения чистого уравнения  $x^\beta - T = 0$ , то ясно, что  $T$  в большинстве случаев имеет мнимое значение  $P + iQ$ , так что это уравнение, как известно, связано, с одной стороны, с делением некоторого угла (тангенс которого равен  $Q/P$ ), на  $\beta$  частей, а с другой — с извлечением корня степени  $\beta$  из некоторого отношения (отношения единицы к  $\sqrt{P^2 + Q^2}$ ). При этом весьма замечательно (о чем подробнее мы, однако, говорить не будем), что значение  $\sqrt[\beta]{P^2 + Q^2}$  всегда может быть выражено рационально через уже известные величины, так что, кроме извлечения квадратного корня, для решения уравнения нужно только деление некоторого угла, например, при  $\beta = 3$  — трисекция угла.

Так как, наконец, ничто не мешает положить  $\alpha = 1, \gamma = 1$ , и потому  $\beta = n - 1$ , то ясно, что решение уравнения  $x^n - 1 = 0$  тот-

час же может быть сведено к решению чистого уравнения  $x^{n-1} - T = 0$  степени  $n - 1$ , где  $T$  определяется через корни уравнения  $x^{n-1} - 1 = 0$ . Отсюда при помощи сделанного выше замечания следует, что деление полного круга на  $n$  равных частей требует: 1) деления полного круга на  $n - 1$  частей; 2) деления некоторой другой дуги, которая может быть построена после выполнения первого деления, на  $n - 1$  частей; 3) извлечения одного единственного квадратного корня, причем можно показать, что этим корнем всегда является  $\sqrt{n}$ .

### Применение предыдущих исследований к тригонометрическим функциям.

#### Метод различать углы, которым соответствуют отдельные корни из $\Omega$

361

Теперь мы еще рассмотрим подробнее связь между корнями  $\Omega$  и тригонометрическими функциями углов  $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \dots, \frac{(n-1)P}{n}$ . Метод нахождения корней из  $\Omega$ , который мы изложили, таков, что мы еще не можем различать (если не использовать в процессе вычислений указанным выше образом таблиц синусов, что, однако, было бы менее прямым способом), какой корень соответствует каждому из указанных углов, т. е. какой корень равен  $\cos \frac{P}{n} + i \sin \frac{P}{n}$ , какой равен  $\cos \frac{2P}{n} + i \sin \frac{2P}{n}$ , и т. д. Эта неопределенность, однако, легко устраняется, если принять во внимание, что косинусы углов  $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \dots, \frac{(n-1)P}{2n}$  все время убывают (если принимать во внимание и знак), а синусы всех этих углов положительны; углы  $\frac{(n-1)P}{n}, \frac{(n-2)P}{n}, \frac{(n-3)P}{n}, \dots, \frac{(n+1)P}{2n}$  имеют соответственно такие же косинусы, что и углы первого ряда, а синусы углов второго ряда отрицательны, но по абсолютной величине равны синусам углов первого ряда. Поэтому среди корней  $\Omega$  те два, которые имеют наибольшие вещественные (равные между собой) части, соответствуют углам  $\frac{P}{n}, \frac{(n-1)P}{n}$ , причем первому



углу соответствует тот корень, у которого мнимая величина  $i$  умножается на положительную величину, а второму — тот, у которого она умножается на отрицательную величину. Из остальных  $n - 3$  корней те, которые имеют наибольшие вещественные части, соответствуют углам  $\frac{2P}{n}$ ,  $\frac{(n-2)P}{n}$  и т. д. Если корень, который соответствует углу  $\frac{P}{n}$ , уже известен, то остальные можно еще различать и на основании того, что если указанный корень обозначить через  $[\lambda]$ , то углам  $\frac{2P}{n}$ ,  $\frac{3P}{n}$ ,  $\frac{4P}{n}$ , ... будут, очевидно, соответствовать корни  $[2\lambda]$ ,  $[3\lambda]$ ,  $[4\lambda]$ , ... Так, в примере п. 353 тотчас же видно, что углу  $\frac{1}{19}P$  не может соответствовать никакой другой корень, кроме  $[11]$ , а углу  $\frac{18}{19}P$  — никакой другой корень, кроме  $[8]$ ; углам же  $\frac{2}{19}P$ ,  $\frac{17}{19}P$ ,  $\frac{3}{19}P$ ,  $\frac{16}{19}P$ , ... отвечают соответственно корни  $[3]$ ,  $[16]$ ,  $[14]$ ,  $[5]$ , .... В примере п. 354 углу  $\frac{1}{17}P$  соответствует, очевидно, корень  $[1]$ , углу  $\frac{2}{17}P$  — корень  $[3]$  и т. д. Таким образом, косинусы и синусы углов  $\frac{P}{n}$ ,  $\frac{2P}{n}$ , ... полностью определяются.

**Тангенсы, котангенсы, секансы и косекансы  
определяются по синусам и косинусам  
без помощи деления**

362

Что же касается остальных тригонометрических функций этих углов, то их можно было бы определить через синус и косинус известным методом, именно, секанс и тангенс — определить, деля соответственно единицу и синус на косинус, а косеканс и котангенс — деля соответственно единицу и косинус на синус. Однако в большинстве случаев удобнее определять эти функции при помощи следующих формул, в которых не фигурирует деление, а имеется только сложение.

Пусть  $\omega$  — один из углов  $\frac{P}{n}, \frac{2P}{n}, \dots, \frac{(n-1)P}{n}$ , и  $\cos \omega + i \sin \omega = R$ , так что  $R$  есть некоторый корень из  $\Omega$ ; тогда

$$\cos \omega = \frac{1}{2} \left( R + \frac{1}{R} \right) = \frac{1+R^2}{2R}, \quad \sin \omega = \frac{1}{2i} \left( R - \frac{1}{R} \right) = i \frac{1-R^2}{2R}.$$

Отсюда следует, что

$$\sec \omega = \frac{2R}{1+R^2}, \quad \operatorname{tg} \omega = \frac{i(1-R^2)}{1+R^2}, \quad \operatorname{cosec} \omega = \frac{2Ri}{R^2-1}, \quad \operatorname{ctg} \omega = \frac{i(R^2+1)}{R^2-1}$$

Покажем теперь, что числители этих четырех дробей можно так преобразовать, что они станут делящимися на знаменатели.

I. В силу  $R = R^{n+1} = R^{2n+1}$  имеет место  $2R = R + R^{2n+1}$ , а это выражение, очевидно, делится на  $1+R^2$ , так как число  $n$  нечетно. Отсюда получается

$$\sec \omega = R - R^3 + R^5 - R^7 + \dots + R^{2n-1},$$

и потому (так как из  $\sin \omega = -\sin(2n-1)\omega$ ,  $\sin 3\omega = -\sin(2n-3)\omega$ ,  $\dots$ , очевидно, следует  $\sin \omega - \sin 3\omega + \sin 5\omega - \dots + \sin(2n-1)\omega = 0$ )

$$\sec \omega = \cos \omega - \cos 3\omega + \cos 5\omega - \dots + \cos(2n-1)\omega,$$

или, наконец (в силу  $\cos \omega = \cos(2n-1)\omega$ ,  $\cos 3\omega = \cos(2n-3)\omega$ ,  $\dots$ ),

$$\sec \omega = 2 [\cos \omega - \cos 3\omega + \cos 5\omega - \dots \mp \cos(n-2)\omega] \pm \cos n\omega,$$

где нужно брать верхние или нижние знаки, в зависимости от того, имеет ли  $n$  вид  $4k+1$  или  $4k+3$ . Очевидно, эта формула может быть также представлена в виде

$$\sec \omega = \pm [1 - 2 \cos 2\omega + 2 \cos 4\omega - \dots \pm 2 \cos(n-1)\omega].$$

II. Если подобным же образом подставить  $1 - R^{2n+2}$  вместо  $1 - R^2$ , то получится, что

$$\operatorname{tg} \omega = i(1 - R^2 + R^4 - R^6 + \dots - R^{2n}),$$

или (так как  $1 - R^{2n} = 0$ ,  $R^2 - R^{2n-2} = 2i \sin 2\omega$ ,  $R^4 - R^{2n-4} = 2i \sin 4\omega$ ,  $\dots$ )

$$\operatorname{tg} \omega = 2 [\sin 2\omega - \sin 4\omega + \sin 6\omega - \dots \mp \sin(n-1)\omega].$$

III. Так как имеет место  $1 + R^2 + R^4 + \dots + R^{2n-2} = 0$ , то

$$\begin{aligned} n &= n - 1 - R^2 - R^4 - \dots - R^{2n-2} = \\ &= (1 - 1) + (1 - R^2) + (1 - R^4) + \dots + (1 - R^{2n-2}), \end{aligned}$$

и отдельные скобки этого выражения делятся на  $1 - R^2$ . Поэтому

$$\begin{aligned} \frac{n}{1 - R^2} &= 1 + (1 + R^2) + (1 + R^2 + R^4) + \dots + (1 + R^2 + R^4 + \dots \\ &\dots + R^{2n-4}) = (n - 1) + (n - 2)R^2 + (n - 3)R^4 + \dots + R^{2n-4}, \end{aligned}$$

откуда, умножая на 2, вычитая затем

$$0 = (n - 1)(1 + R^2 + R^4 + \dots + R^{2n-2})$$

и снова умножая на  $R$ , мы получаем

$$\begin{aligned} \frac{2nR}{1 - R^2} &= (n - 1)R + (n - 3)R^3 + (n - 5)R^5 + \dots - (n - 3)R^{2n-3} - \\ &\dots - (n - 1)R^{2n-1}, \end{aligned}$$

откуда тотчас же следует, что

$$\begin{aligned} \operatorname{cosec} \omega &= \frac{1}{n} [(n - 1) \sin \omega + (n - 3) \sin 3\omega + \dots - (n - 1) \sin (2n - 1) \omega] = \\ &= \frac{2}{n} [(n - 1) \sin \omega + (n - 3) \sin 3\omega + \dots + 2 \sin (n - 2) \omega], \end{aligned}$$

причем эта формула может быть представлена также и в виде

$$\operatorname{cosec} \omega = -\frac{2}{n} [2 \sin 2\omega + 4 \sin 4\omega + 6 \sin 6\omega + \dots + (n - 1) \sin (n - 1) \omega].$$

IV. Если указанное выше значение  $n/(1 - R^2)$  умножить на  $1 + R^2$  и затем вычесть

$$0 = (n - 1)(1 + R^2 + R^4 + \dots + R^{2n-2}),$$

то получится

$$\frac{n(1 + R^2)}{1 - R^2} = (n - 2)R^2 + (n - 4)R^4 + (n - 6)R^6 + \dots - (n - 2)R^{2n-2},$$

откуда тотчас же следует, что

$$\begin{aligned} \operatorname{ctg} \omega &= \frac{1}{n} [(n - 2) \sin 2\omega + (n - 4) \sin 4\omega + (n - 6) \sin 6\omega + \dots \\ &\dots - (n - 2) \sin (n - 2) \omega] = \frac{2}{n} [(n - 2) \sin 2\omega + \\ &+ (n - 4) \sin 4\omega + \dots + 3 \sin (n - 3) \omega + \sin (n - 1) \omega], \end{aligned}$$

причем эту формулу можно представить также и в виде

$$\operatorname{ctg} \omega = -\frac{2}{n} [\sin \omega + 3 \sin 3\omega + \dots + (n - 2) \sin (n - 2) \omega].$$

## Метод постепенного понижения степеней уравнений для тригонометрических функций

363

Точно так же, как при предположении, что  $n - 1 = ef$ , функция  $X$  может быть разложена на  $e$  сомножителей степени  $f$ , если известны значения всех  $e$  сумм из  $f$  членов (п. 348), так и для уравнения  $Z = 0$  степени  $n - 1$ , корнями которого являются синусы или какие-либо другие тригонометрические функции углов  $\frac{P}{n}, \frac{2P}{n}, \dots, \frac{(n-1)P}{n}$ , функция  $Z$  может быть тогда разложена на  $e$  сомножителей степени  $f$ . Основные моменты этого способа состоят в следующем.

Пусть  $\Omega$  состоит из следующих  $e$  периодов по  $f$  членов:  $(f, 1) = P, P', P'', \dots$ , и период  $P$  состоит из корней  $[1], [a], [b], [c], \dots$ , период  $P'$  — из корней  $[a'], [b'], [c'], \dots$ , период  $P''$  — из корней  $[a''], [b''], [c''], \dots$ . Пусть, далее, корню  $[1]$  соответствует угол  $\omega$ , и потому корням  $[a], [b], \dots$  — углы  $a\omega, b\omega, \dots$ , корням  $[a'], [b'], \dots$  — углы  $a'\omega, b'\omega, \dots$ , корням  $[a''], [b''], \dots$  — углы  $a''\omega, b''\omega, \dots$  и т. д. Тогда легко видеть, что все эти углы совпадают с углами  $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \dots, \frac{(n-1)P}{n}$ , точнее, что совпадают тригонометрические функции первых и вторых\*. Поэтому, если обозначить тригонометрическую функцию, о которой идет речь, буквой  $\varphi$ , ставящейся перед значением угла, и положить произведение сомножителей

$$x - \varphi(\omega), \quad x - \varphi(a\omega), \quad x - \varphi(b\omega), \dots$$

равным  $Y$ , произведение сомножителей  $x - \varphi(a'\omega), x - \varphi(b'\omega), \dots$  равным  $Y'$ , произведение сомножителей  $x - \varphi(a''\omega), x - \varphi(b''\omega), \dots$  равным  $Y''$  и т. д., то, очевидно, будет иметь место  $YY'Y'' \dots = Z$ . Нам еще нужно только показать, что все коэффициенты функций  $Y, Y', Y'', \dots$  могут быть представлены в виде

$$A + B(f, 1) + C(f, g) + D(f, g^2) + \dots + L(f, g^{e-1}),$$

---

\* В этом смысле два угла совпадают, если разность между ними равна или полной окружности, или некоторой ее кратности; такие углы можно было бы назвать сравнимыми по полной окружности, если понимать сравнимость в несколько расширенном смысле.

вследствие чего их, очевидно, можно будет считать известными, если известны значения всех сумм из  $f$  членов. Этого мы добиваемся следующим образом.

Подобно тому как

$$\cos \omega = \frac{1}{2} [1] + \frac{1}{2} [1]^{n-1}, \quad \sin \omega = -\frac{1}{2} i [1] + \frac{1}{2} i [1]^{n-1},$$

так же и остальные тригонометрические функции угла  $\omega$  могут быть приведены к виду  $\mathfrak{A} + \mathfrak{B} [1] + \mathfrak{C} [1]^2 + \mathfrak{D} [1]^3 + \dots$ , и непосредственно ясно, что если  $k$  обозначает некоторое целое число, то функции угла  $k\omega$  будут тогда равны  $\mathfrak{A} + \mathfrak{B} [k] + \mathfrak{C} [k]^2 + \dots + \mathfrak{D} [k]^3 + \dots$ . Но так как отдельные коэффициенты у  $Y$  являются целыми рациональными симметрическими функциями от  $\varphi(\omega)$ ,  $\varphi(a\omega)$ ,  $\varphi(b\omega)$ ,  $\dots$ , то ясно, что если вместо этих величин подставить их значения, то отдельные коэффициенты станут целыми рациональными симметрическими функциями от  $[1]$ ,  $[a]$ ,  $[b]$ ,  $\dots$ , вследствие чего они, согласно п. 347, приводятся к виду  $A + B(f, 1) + \dots + C(f, g) + \dots$ . И по совершенно той же причине возможно привести к подобному виду и все коэффициенты функций  $Y'$ ,  $Y''$ ,  $\dots$ .

### 364

*Относительно проблемы предыдущего пункта мы добавим еще несколько замечаний.*

I. Так как отдельные коэффициенты у  $Y'$  являются такими же функциями от содержащихся в периоде  $P'$  (который можно обозначить через  $(f, a')$ ) корней, что и отдельные коэффициенты у  $Y$  как функции корней из  $P$ , то из п. 347 вытекает, что  $Y'$  получается из  $Y$ , если в выражении для  $Y$  вместо  $(f, 1)$ ,  $(f, g)$ ,  $(f, g^2)$ ,  $\dots$  всюду подставить соответственно  $(f, a')$ ,  $(f, a'g)$ ,  $(f, a'g^2)$ ,  $\dots$ . И точно так же  $Y''$  получается из  $Y$ , если в выражении для  $Y$  всюду вместо  $(f, 1)$ ,  $(f, g)$ ,  $(f, g^2)$ ,  $\dots$  подставить соответственно  $(f, a'')$ ,  $(f, a''g)$ ,  $(f, a''g^2)$ ,  $\dots$ . Поэтому если функция  $Y$  найдена, то остальные функции  $Y'$ ,  $Y''$ ,  $\dots$  получаются немедленно из нее.

II. Если мы положим

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \dots,$$

то коэффициенты  $\alpha$ ,  $\beta$ ,  $\dots$  будут соответственно равны сумме корней

уравнения  $Y = 0$ , т. е. сумме величин  $\varphi(\omega)$ ,  $\varphi(a\omega)$ ,  $\varphi(b\omega)$ , ..., сумме произведений этих величин по две и т. д. Однако в большинстве случаев намного удобнее искать эти коэффициенты при помощи метода, подобного указанному в п. 349, а именно, сначала найти сумму корней  $\varphi(\omega)$ ,  $\varphi(a\omega)$ ,  $\varphi(b\omega)$ , ..., сумму их квадратов, сумму кубов и т. д., а затем получить коэффициенты при помощи теоремы Ньютона. Если  $\varphi$  обозначает тангенс, секанс, котангенс или косеканс, то существуют еще и другие вспомогательные средства, о которых, однако, мы здесь не будем говорить.

III. Особого рассмотрения заслуживает тот случай, когда  $f$  является четным числом, и потому каждый период  $P$ ,  $P'$ ,  $P''$ , ... составлен из  $\frac{1}{2}f$  периодов по два члена. Если  $P$  состоит из периодов  $(2, 1)$ ,  $(2, a)$ ,  $(2, b)$ ,  $(2, c)$ , ..., то числа  $1, a, b, c, \dots$  и  $n-1$ ,  $n-a$ ,  $n-b$ ,  $n-c, \dots$  вместе составляют всю совокупность  $1, a, b, c, \dots$  или по крайней мере (что здесь сводится к тому же) сравнимы с последними числами по модулю  $n$ . Но  $\varphi((n-1)\omega) = \pm \varphi(\omega)$ ,  $\varphi((n-a)\omega) = \pm \varphi(a\omega)$ , и т. д., где нужно брать верхние знаки, если  $\varphi$  обозначает косинус или секанс и нижние знаки, если  $\varphi$  обозначает синус, тангенс, котангенс или косеканс. Отсюда следует, что в *обоих первых случаях* сомножители, из которых состоит  $Y$ , разбиваются на пары равных между собой, и потому  $Y$  является квадратом, а именно,  $Y = y^2$ , где  $y$  равно произведению сомножителей

$$x - \varphi(\omega), \quad x - \varphi(a\omega), \quad x - \varphi(b\omega), \dots$$

Точно так же в этих случаях и остальные функции  $Y'$ ,  $Y''$  ... являются квадратами, причем, если мы предположим, что  $P'$  состоит из  $(2, a')$ ,  $(2, b')$ ,  $(2, c')$ , ...,  $P''$  — из  $(2, a'')$ ,  $(2, b'')$ ,  $(2, c'')$ , ... и т. д., и что произведение сомножителей  $x - \varphi(a'\omega)$ ,  $x - \varphi(b'\omega)$ ,  $x - \varphi(c'\omega)$ , ... равно  $y'$ , произведение сомножителей  $x - \varphi(a''\omega)$ ,  $x - \varphi(b''\omega)$ , ... равно  $y''$  и т. д., то  $Y' = y'^2$ ,  $Y'' = y''^2$  и т. д. Далее, функция  $Z$  также является квадратом (ср. п. 337), а именно, квадратом произведения  $yy'y'', \dots$ . Легко видеть также, что  $y'$ ,  $y'', \dots$  точно так же получаются из  $y$ , как  $Y'$ ,  $Y'', \dots$  получаются, согласно сказанному в I, из  $Y$ ; что отдельные коэффициенты у  $y$

могут быть представлены в виде

$$A + B(f, 1) + C(f, g) + \dots,$$

так как суммы отдельных степеней корней уравнения  $y = 0$ , очевидно, равны половинам сумм степеней корней уравнения  $Y = 0$  и потому приводятся к такому виду.

В четырех последних случаях  $Y$  является произведением сомножителей

$$x^2 - (\varphi(\omega))^2, \quad x^2 - (\varphi(a\omega))^2, \quad x^2 - (\varphi(b\omega))^2, \dots$$

и потому имеет вид

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \dots$$

и ясно, что коэффиценты  $\lambda, \mu, \dots$  могут быть получены из сумм квадратов, биквадратов и т. д. корней  $\varphi(\omega), \varphi(a\omega), \varphi(b\omega), \dots$ ; так же обстоит дело и с функциями  $Y', Y'', \dots$

**Пример I.** Пусть  $n = 17$ ,  $f = 8$ , и  $\varphi$  обозначает косинус. Тогда

$$Z = \left( x^8 + \frac{1}{2} x^7 - \frac{7}{4} x^6 - \frac{3}{4} x^5 + \frac{15}{16} x^4 + \frac{5}{16} x^3 - \frac{5}{32} x^2 - \frac{1}{32} x + \frac{1}{256} \right)^2,$$

и нужно разложить  $\sqrt{Z}$  на два сомножителя  $y, y'$  четвертой степени. Период  $P = (8, 1)$  состоит из  $(2, 1), (2, 9), (2, 13), (2, 15)$ , поэтому  $y$  будет произведением сомножителей

$$x - \varphi(\omega), \quad x - \varphi(9\omega), \quad x - \varphi(13\omega), \quad x - \varphi(15\omega).$$

Если вместо  $\varphi(k\omega)$  подставить  $\frac{1}{2}[k] + \frac{1}{2}[n - k]$ , мы найдем

$$\varphi(\omega) + \varphi(9\omega) + \varphi(13\omega) + \varphi(15\omega) = \frac{1}{2}(8, 1);$$

$$(\varphi(\omega))^2 + (\varphi(9\omega))^2 + (\varphi(13\omega))^2 + (\varphi(15\omega))^2 = 2 + \frac{1}{4}(8, 1);$$

точно так же сумма кубов равна  $\frac{3}{8}(8, 1) + \frac{1}{8}(8, 3)$ , сумма биквадратов равна  $\frac{3}{2} + \frac{5}{16}(8, 1)$ . Определяя отсюда по теореме Ньютона коэффиценты функции  $y$ , мы получим

$$y = x^4 - \frac{1}{2}(8, 1)x^3 + \frac{1}{4}[(8, 1) + 2(8, 3)]x^2 - \frac{1}{8}[(8, 1) + 3(8, 3)]x + \frac{1}{16}[(8, 1) + (8, 3)];$$

$y'$  получается из  $y$ , если поменять местами  $(8, 1)$  и  $(8, 3)$ . Если подставить теперь вместо  $(8, 1)$  и  $(8, 3)$  значения  $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$  и  $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$ , то мы получим

$$y = x^4 + \left(\frac{1}{4} - \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} + \frac{1}{8}\sqrt{17}\right)x^2 + \left(\frac{1}{4} + \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16},$$

$$y' = x^4 + \left(\frac{1}{4} + \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} - \frac{1}{8}\sqrt{17}\right)x^2 + \left(\frac{1}{4} - \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16}.$$

Подобным же образом можно разложить  $\sqrt{Z}$  на четыре сомножителя второй степени, первый из которых  $(x - \varphi(\omega))(x - \varphi(13\omega))$ , второй  $(x - \varphi(9\omega))(x - \varphi(15\omega))$ , третий есть  $(x - \varphi(3\omega))(x - \varphi(5\omega))$ , и четвертый  $(x - \varphi(10\omega))(x - \varphi(11\omega))$ , и все коэффициенты этих сомножителей могут быть выражены через четыре суммы  $(4, 1)$ ,  $(4, 9)$ ,  $(4, 3)$ ,  $(4, 10)$ . Очевидно, что произведение первого и второго сомножителей будет равно  $y$ , а произведение третьего и четвертого равно  $y'$ .

**Пример II.** Если  $\varphi$  обозначает синус, а все остальное остается без изменения, так что

$$Z = x^{16} - \frac{17}{4}x^{14} + \frac{119}{16}x^{12} - \frac{221}{32}x^{10} + \frac{935}{256}x^8 - \frac{561}{512}x^6 + \frac{357}{2048}x^4 - \frac{51}{4096}x^2 + \frac{17}{65536}$$

нужно разложить на два сомножителя  $y$ ,  $y'$  восьмой степени, то  $y$  будет произведением четырех двойных сомножителей

$$x^2 - (\varphi(\omega))^2, \quad x^2 - (\varphi(9\omega))^2, \quad x^2 - (\varphi(13\omega))^2, \quad x^2 - (\varphi(15\omega))^2.$$

Но так как  $\varphi(k\omega) = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$ , то

$$(\varphi(k\omega))^2 = -\frac{1}{4}[2k] + \frac{1}{2}[n] - \frac{1}{4}[2n-2k] = \frac{1}{2} - \frac{1}{4}[2k] - \frac{1}{4}[2n-2k].$$

Отсюда для суммы квадратов корней  $\varphi(\omega)$ ,  $\varphi(9\omega)$ ,  $\varphi(13\omega)$ ,  $\varphi(15\omega)$  мы находим значение  $2 - \frac{1}{4}(8, 1)$ , для суммы их биквадратов — значение  $\frac{3}{2} - \frac{3}{16}(8, 1)$ , для суммы их шестых степеней — значение  $\frac{5}{4} - \frac{9}{64}(8, 1) - \frac{1}{64}(8, 3)$ , и для их суммы восьмых степеней — значение  $\frac{35}{32} - \frac{27}{256}(8, 1) - \frac{1}{32}(8, 3)$ .



Отсюда следует:

$$y = x^8 - \left[ 2 - \frac{1}{4} (8,1) \right] x^6 + \left[ \frac{3}{2} - \frac{5}{16} (8,1) + \frac{1}{8} (8,3) \right] x^4 - \\ - \left[ \frac{1}{2} - \frac{9}{64} (8,1) + \frac{5}{64} (8,3) \right] x^2 + \frac{1}{16} - \frac{5}{256} (8,1) + \frac{3}{256} (8,3),$$

а  $y'$  получается из  $y$  перестановкой  $(8,1)$  и  $(8,3)$ , так что, подставляя значения этих сумм, мы получаем

$$y = x^8 - \left( \frac{17}{8} - \frac{1}{8} \sqrt{17} \right) x^6 + \left( \frac{51}{32} - \frac{7}{32} \sqrt{17} \right) x^4 - \\ - \left( \frac{17}{32} - \frac{7}{64} \sqrt{17} \right) x^2 + \frac{17}{256} - \frac{1}{64} \sqrt{17}, \\ y' = x^8 - \left( \frac{17}{8} + \frac{1}{8} \sqrt{17} \right) x^6 + \left( \frac{51}{32} + \frac{7}{32} \sqrt{17} \right) x^4 - \left( \frac{17}{32} + \frac{7}{64} \sqrt{17} \right) x^2 + \\ + \frac{17}{256} + \frac{1}{64} \sqrt{17}.$$

Точно так же можно разложить  $Z$  на четыре сомножителя, коэффициенты которых могут быть выражены через суммы из четырех членов, причем произведение двух будет равно  $y$ , а произведение двух других равно  $y'$ .

**Деления круга, которые можно выполнить  
при помощи квадратных уравнений  
или посредством геометрических построений**

### 365

Таким образом, предыдущими исследованиями мы свели деление круга на  $n$  равных частей, где  $n$  есть простое число, к решению уравнений число которых равно количеству сомножителей, на которые может быть разложено число  $n-1$ , а степени уравнений определяются величиной сомножителей. Поэтому, если  $n-1$  есть степень числа 2, что имеет место для значений  $n = 3, 5, 17, 257, 65537, \dots$ , то деление круга сводится к решению только квадратных уравнений, и тригонометрические функции углов  $P/n, 2P/n, \dots$  могут быть выражены через более или менее сложные (в зависимости от величины  $n$ ) квадратные уравнения. Следова-

тельно, в этом случае деление круга на  $n$  равных частей или построение правильного  $n$ -угольника может быть выполнено при помощи геометрических построений. Например, для  $n = 17$  из пп. 354, 361 для косинуса угла  $\frac{1}{17}P$  легко выводится следующее выражение:

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \\ + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Косинусы кратностей этого угла имеют аналогичный вид, синусы же содержат на один радикал больше. Весьма замечательно, что в то время как возможность геометрического деления круга на три и пять частей была известна уже ко временам Эвклида, к этим сведениям на протяжении 2000 лет не было добавлено ничего нового, и что все математики считали, что кроме указанных делений, и тех, которые непосредственно получаются из них, именно, делений на 15,  $3 \cdot 2^u$ ,  $5 \cdot 2^u$ ,  $15 \cdot 2^u$  и  $2^u$  частей, никакие другие деления при помощи геометрических построений не выполнимы. Легко доказать, впрочем, что если  $n = 2^m + 1$  есть простое число, то и показатель  $m$  не может содержать никаких простых сомножителей, кроме числа 2, и потому равен либо 1, либо 2, либо более высокой степени числа 2; действительно, если бы  $m$  делилось на некоторое нечетное число  $\zeta$  (большее чем 1), и именно, имело бы место  $m = \zeta\eta$ , то  $2^m + 1$  делилось бы на  $2^\eta + 1$  и потому было бы составным числом. Таким образом, все значения  $n$ , для которых получаются только квадратные уравнения, представляются в виде  $2^{2^v} + 1$ ; таким образом, получаются пять чисел 3, 5, 17, 257, 65537, если полагать  $v = 0, 1, 2, 3, 4$  или  $m = 1, 2, 4, 8, 16$ . Однако геометрическое деление круга можно провести ни в коем случае не для всех чисел такого вида, а лишь для тех из них, которые являются простыми. Правда, Ферма утверждал из индуктивных соображений, что все числа такого вида обязательно являются простыми; однако Эйлер впервые заметил, что уже для  $v = 5$  или  $m = 32$  это правило оказывается неверным, так как число  $2^{32} + 1 = 4294967297$  содержит сомножитель 641.

Если же  $n - 1$  содержит, кроме числа 2, другие простые сомножители, то мы всегда приходим к уравнениям более высокой степени, именно, к одному или нескольким кубическим, если число 3 содержится один или несколько раз среди сомножителей числа  $n - 1$ , к уравнениям пятой степени, если  $n - 1$  делится на 5 и т. д., и мы можем со всей строгостью доказать, что эти уравнения более высоких степеней никак не могут быть исключены или сведены к уравнениям более низкой степени; хотя границы настоящего сочинения не позволяют привести здесь это доказательство, мы считаем своим долгом указать на это, чтобы никто не надеялся бы свести еще и другие деления кроме делений, дающихся нашей теорией, например, деления на 7, 11, 13, 19, ... частей к геометрическим построениям, и не тратил бы бесполезно свое время.

## 366

Если нужно разделить круг на  $a^\alpha$  частей, где  $a$  обозначает простое число, то это, очевидно, всегда можно сделать геометрически, если  $a = 2$ , но ни для каких других значений  $a$  это уже невозможно, если только  $\alpha > 1$ ; действительно, нам тогда пришлось бы решать, кроме тех уравнений, которые нужны для деления на  $a$  частей, также и  $\alpha - 1$  других уравнений степени  $a$ ; эти уравнения также не могут быть исключены или понижены. Степени необходимых уравнений, таким образом, всегда (т. е. также и для случая  $\alpha = 1$ ) будут равны простым сомножителям числа  $(a - 1) a^{\alpha-1}$ .

Если, наконец, нужно разделить круг на  $N = a^\alpha b^\beta c^\gamma \dots$  частей, где  $a, b, c, \dots$  обозначают различные простые числа, то достаточно уметь производить деление на  $a^\alpha, b^\beta, c^\gamma, \dots$  частей (п. 336) поэтому, чтобы узнать степени требуемых для этой цели уравнений, нужно рассмотреть простые сомножители чисел

$$(a - 1) a^{\alpha-1}, (b - 1) b^{\beta-1}, (c - 1) c^{\gamma-1}, \dots,$$

или, что сводится к тому же, произведения этих чисел. Заметим, что это произведение выражает количество чисел, которые взаимно просты с  $N$  и меньше чем  $N$  (п. 38). Таким образом, геометрически деление можно произвести только тогда, когда это число есть степень числа 2;

если же оно, кроме 2, содержит еще и другие простые сомножители, например,  $p, p', \dots$ , то от уравнений  $p$ -й,  $p'$ -й и т. д. степеней никаким образом нельзя будет избавиться. Отсюда мы заключаем вообще, что для того, чтобы круг можно было геометрически разделить на  $N$  частей, нужно, чтобы  $N$  было равно либо 2, либо более высокой степени числа 2, или чтобы  $N$  было либо простым числом вида  $2^m + 1$ , либо произведением нескольких таких простых чисел, или чтобы  $N$  было произведением одного или нескольких таких простых чисел либо на 2, либо на более высокую степень числа 2; короче говоря, необходимо, чтобы  $N$  не содержало никаких нечетных простых сомножителей, кроме имеющих вид  $2^m + 1$ , и никакого сомножителя указанного вида не содержало в степени выше первой. Среди чисел до 300 такими значениями  $N$  являются следующие 38: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272 \*.

---

\* Если бы все числа вида  $2^{2^m} + 1$  были простыми, то достаточно точным выражением для количества рассматриваемых чисел ( $N$ ), меньших заданного числа  $M$ , было бы  $\frac{1}{2} \left( \frac{\log M}{\log 2} \right)^2$ .

---

## ДОПОЛНЕНИЯ

К п. 28. Решение неопределенного уравнения  $ax = by \pm 1$  было впервые дано не Эйлером (как сказано в тексте), а уже одним математиком семнадцатого столетия, Баше де Мезириаком, замечательным издателем и комментатором Диофанта, и эту честь признал за ним Лагранж («*Add. a l'Algèbre d'Euler*», p. 525, где одновременно указывается сущность метода). Баше изложил свое открытие во втором издании своей книги «*Problèmes plaisans et délectables qui se font par les nombres*»; в первом издании, с которым я только и мог ознакомиться, его еще нет, хотя оно уже и было сделано.

К п. 151, 296, 297. Лежандр заново изложил свое доказательство в замечательном сочинении «*Essai d'une théorie des nombres*», однако по существу ничего в нем не изменил, поэтому все возражения против его метода, приведенные в п. 297, остаются в силе. Хотя теорема (на которой основывается одно предположение) о том, что в каждой арифметической прогрессии  $l, l + k, l + 2k, \dots$  имеются простые числа, если только  $l$  и  $k$  не имеют общих делителей, в этом сочинении рассматривается подробнее, но в смысле математической строгости сделанного еще не достаточно. Однако, если бы эта теорема и была полностью доказана, остается еще одно предположение (что имеются простые числа вида  $4n + 3$ , по которым заданное положительное простое число вида  $4n + 1$  является квадратичным невычетом), и я не знаю, можно ли его строго доказать, не предполагая уже известной саму фундаментальную теорему. Впрочем, надо заметить, что Лежандр делает это предположение не молчаливо, а и сам обращает на него внимание.

К пп. 288—293. Относительно того вопроса, который здесь рассматривается как специальное приложение теории тройничных форм, и который должен быть разобран так, чтобы в отношении строгости и общности не оставалось желать ничего лучшего, Лежандр в третьем разделе своего сочинения проводит намного более подробное исследование\*. При этом он использует принципы, совершенно отличные от наших; однако на этом пути он столкнулся со многими трудностями, в результате чего не смог обосновать основные теоремы строгими доказательствами. На эти трудности он сам честно указал; однако, если мы не ошибаемся, они могут быть устранены легче, чем та, что в этом исследовании предполагается справедливой упомянутая выше теорема («В каждой геометрической прогрессии и т. д.»).

К п. 306, VIII. В третьей тысяче отрицательных определителей имеется 37 иррегулярных, из которых 18 имеют показатель иррегулярности 2, остальные 19 — показатель иррегулярности 3.

К п. 306, X. Недавно нам посчастливилось полностью решить поставленную здесь задачу; это исследование, которое поразительным образом проливает свет на многие вопросы как высшей арифметики, так и анализа, мы при первой возможности опубликуем как продолжение настоящего сочинения. Результат состоит в том, что коэффициент  $m$  из п. 304 равен  $\gamma\pi \approx 2,3458847616$ , где  $\gamma$  обозначает ту же величину, что и в п. 302, а  $\pi$ , как и там, обозначает половину длины окружности радиуса 1.

---

\* Хотя мы на это и не указываем, читатель не должен смешивать наши тройничные формы с тем, что Лежандр называет «forme trinaire d'un nombre». Именно, под этим выражением он понимает разложение числа на три квадрата.

---

Таблица 1 (пп. 58,91)

|    | 1  | 2  | 3  | 5  | 7  | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 71 | 73 | 79 | 83 | 89 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 3  | 2  | 1  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 5  | 2  | 1  | 3  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 7  | 3  | 2  | 1  | 5  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 9  | 2  | 1  | *  | 5  | 4  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 11 | 2  | 1  | 8  | 4  | 7  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 13 | 6  | 5  | 8  | 9  | 7  | 11 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 16 | 5  | *  | 3  | 1  | 2  | 1  | 3  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 17 | 10 | 10 | 11 | 7  | 9  | 13 | 12 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 19 | 10 | 17 | 5  | 2  | 12 | 6  | 13 | 8  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 23 | 10 | 8  | 20 | 15 | 21 | 3  | 12 | 17 | 5  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 25 | 2  | 1  | 7  | *  | 5  | 16 | 19 | 13 | 18 | 11 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 27 | 2  | 1  | *  | 5  | 16 | 13 | 8  | 15 | 12 | 11 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 29 | 10 | 11 | 27 | 18 | 20 | 23 | 2  | 7  | 15 | 24 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 31 | 17 | 12 | 13 | 20 | 4  | 29 | 23 | 1  | 22 | 21 | 27 |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 32 | 5  | *  | 3  | 1  | 2  | 5  | 7  | 4  | 7  | 6  | 3  | 0  |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 37 | 5  | 11 | 34 | 1  | 28 | 6  | 13 | 5  | 25 | 21 | 15 | 27 |    |    |    |    |    |    |    |    |    |    |    |    |    |
| 41 | 6  | 26 | 15 | 22 | 39 | 3  | 31 | 33 | 9  | 36 | 7  | 28 | 32 |    |    |    |    |    |    |    |    |    |    |    |    |
| 43 | 28 | 39 | 17 | 5  | 7  | 6  | 40 | 16 | 29 | 20 | 25 | 32 | 35 | 18 |    |    |    |    |    |    |    |    |    |    |    |
| 47 | 10 | 30 | 18 | 17 | 38 | 27 | 3  | 42 | 29 | 39 | 43 | 5  | 24 | 25 | 37 |    |    |    |    |    |    |    |    |    |    |
| 49 | 10 | 2  | 13 | 41 | *  | 16 | 9  | 31 | 35 | 32 | 24 | 7  | 38 | 27 | 36 | 23 |    |    |    |    |    |    |    |    |    |
| 53 | 26 | 25 | 9  | 31 | 38 | 46 | 28 | 42 | 41 | 39 | 6  | 45 | 22 | 33 | 30 | 8  |    |    |    |    |    |    |    |    |    |
| 59 | 10 | 25 | 32 | 34 | 44 | 45 | 23 | 14 | 22 | 27 | 4  | 7  | 41 | 2  | 13 | 53 | 28 |    |    |    |    |    |    |    |    |
| 61 | 10 | 47 | 42 | 14 | 23 | 45 | 20 | 49 | 22 | 39 | 25 | 13 | 33 | 18 | 41 | 40 | 51 | 17 |    |    |    |    |    |    |    |
| 64 | 5  | *  | 3  | 1  | 10 | 5  | 15 | 12 | 7  | 14 | 11 | 8  | 9  | 14 | 13 | 12 | 5  | 1  | 3  |    |    |    |    |    |    |
| 67 | 12 | 29 | 9  | 39 | 7  | 61 | 23 | 8  | 26 | 20 | 22 | 43 | 44 | 19 | 63 | 64 | 3  | 54 | 5  |    |    |    |    |    |    |
| 71 | 62 | 58 | 18 | 14 | 33 | 43 | 27 | 7  | 38 | 5  | 4  | 13 | 30 | 55 | 44 | 17 | 59 | 29 | 37 | 11 |    |    |    |    |    |
| 73 | 5  | 8  | 6  | 1  | 33 | 55 | 59 | 21 | 62 | 46 | 35 | 11 | 64 | 4  | 51 | 31 | 53 | 5  | 58 | 50 | 44 |    |    |    |    |
| 79 | 29 | 50 | 71 | 34 | 19 | 70 | 74 | 9  | 10 | 52 | 1  | 76 | 23 | 21 | 47 | 55 | 7  | 17 | 75 | 54 | 33 | 4  |    |    |    |
| 81 | 11 | 25 | *  | 35 | 22 | 1  | 38 | 15 | 12 | 5  | 7  | 14 | 24 | 29 | 10 | 13 | 45 | 53 | 4  | 20 | 33 | 48 | 52 |    |    |
| 83 | 50 | 3  | 52 | 81 | 24 | 72 | 67 | 4  | 59 | 16 | 36 | 32 | 60 | 38 | 49 | 69 | 13 | 20 | 34 | 53 | 17 | 43 | 47 |    |    |
| 89 | 30 | 72 | 87 | 18 | 7  | 4  | 65 | 82 | 53 | 31 | 29 | 57 | 77 | 67 | 59 | 34 | 10 | 45 | 19 | 32 | 26 | 68 | 46 | 27 |    |
| 97 | 10 | 86 | 2  | 11 | 53 | 82 | 83 | 19 | 27 | 79 | 47 | 26 | 41 | 71 | 44 | 60 | 14 | 65 | 32 | 51 | 25 | 20 | 42 | 91 | 18 |

**Таблица 2 (п. 99)**



Таблица 3 (п. 316)

|    |                                                                                                                                              |
|----|----------------------------------------------------------------------------------------------------------------------------------------------|
| 3  | (0)..3; (1)..6.                                                                                                                              |
| 7  | (0)..142857.                                                                                                                                 |
| 9  | (0)..1; (1)..2; (2)..4; (3)..8; (4)..7; (5)..5.                                                                                              |
| 11 | (0)..09; (1)..18; (2)..36; (3)..72; (4)..45.                                                                                                 |
| 13 | (0)..076923; (1)..461538.                                                                                                                    |
| 17 | (0)..0588235294 117647.                                                                                                                      |
| 19 | (0)..0526315789 47368421.                                                                                                                    |
| 23 | (0)..0434782608 6956521739 13.                                                                                                               |
| 27 | (0)..037; (1)..074; (2)..148; (3)..296; (4)..592; (5)..185.                                                                                  |
| 29 | (0)..0344827586 2068965517 24137931.                                                                                                         |
| 31 | (0)..032280645 16129; (1)..5483870967 74193.                                                                                                 |
| 37 | (0)..027; (1)..135; (2)..675; (3)..378; (4)..891; (5)..459; (6)..297;<br>(7)..486; (8)..432; (9)..162; (10)..810; (11)..054.                 |
| 41 | (0)..02439;(1)..14634;(2)..87804;(3)..26829;(4)..60975;(5)..65853;<br>(6)..95121; (7)..70731.                                                |
| 43 | (0)..0232558139 5348837209 3; (1)..6511627906 9767441860 4.                                                                                  |
| 47 | (0)..0212765957 4468085106 3829787234 0425531914 893617.                                                                                     |
| 49 | (0)..0204081632 6530612244 8979591836 7346938775 51.                                                                                         |
| 53 | (0)..0188679245 283; (1)..4905660377 358; (2)..7547169811 320;<br>(3)..6226415094 339.                                                       |
| 59 | (0)..0169491525 4237288135 5932203389 8305084745 7627118644<br>06779661.                                                                     |
| 61 | (0)..0163934426 2295081967 2131147540 9836065573 7704918032<br>7868852459.                                                                   |
| 67 | (0)..0149253731 3432835820 8955223880 597;<br>(1)..1791044776 1194029850 7462686567 164.                                                     |
| 71 | (0)..0140845070 4225352112 6760563380 28169;<br>(1)..8732394366 1971830985 9154929577 46478.                                                 |
| 73 | (0)..01369863; (1)..06849315; (2)..34246575; (3)..71232876;<br>(4)..56164383; (5)..80821917; (6)..04109589; (7)..20547945;<br>(8)..02739726. |
| 79 | (0)..0126582278 481; (1)..3670886075 949; (2)..6455696202 531;<br>(3)..7215189873 417; (4)..9240506329 113;(5)..7974683544 303.              |

Таблица 3 (п. 316) (окончание)

|    |                                                                                                                   |
|----|-------------------------------------------------------------------------------------------------------------------|
| 81 | (0)..012345679; (1)..135802469; (2)..493827160; (3)..432098765;<br>(4)..753086419; (5)..283950617.                |
| 83 | (0)..0120481927 7108433734 9397590361 4457831325 3,<br>(1)..6024096385 5421686746 9879518072 2891566265 0.        |
| 89 | (0)..0112359550 5617977528 0898876404 4943820224 7191;<br>(1)..3370786516 8539325842 6966292134 8314606741 5730.  |
| 97 | (0)..01030927835051546391 7525773195 87628865979 381443298<br>9690721649 4845360824 7422680412 3711340206 185567. |

---

## О Г Л А В Л Е Н И Е

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Предисловие автора . . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 9         |
| <b>Раздел I. О сравнимости чисел вообще . . . . .</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>15</b> |
| Сравнимые числа, модули, вычеты и невычеты (пп. 1—3). Наименьшие вычеты (п. 4). Элементарные теоремы о сравнениях (п. 5—11). Некоторые приложения (п. 12).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |
| <b>Раздел II. О сравнениях первой степени . . . . .</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>21</b> |
| Предварительные теоремы о простых числах, сомножителях и т. д. (пп. 13—25). Решение сравнений первой степени (пп. 26—31). Нахождение числа, которое сравнимо с заданными вычетами по заданным модулям (пп. 32—36). Линейные сравнения со многими неизвестными (п. 37). Различные теоремы (пп. 38—44).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |
| <b>Раздел III. О степенных вычетах . . . . .</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>50</b> |
| Вычеты членов геометрической прогрессии, начинающейся с единицы, образуют периодический ряд (пп. 45—48). Сначала рассматриваются модули, которые являются простыми числами (пп. 49—81). Теорема Ферма (пп. 50, 51). О количестве чисел, которым соответствуют периоды, у которых количество членов равно заданному делителю числа $p-1$ (пп. 52—56). Первообразные корни, основные числа, индексы (п. 57). Алгоритм индексов (пп. 58, 59). О корнях сравнения $x^n \equiv A$ (пп. 60—68). Связь между индексами в различных системах (пп. 69—71). Основные числа, служащие специальным целям (п. 72). Метод определения первообразных корней (пп. 73, 74). Различные теоремы о периодах и первообразных корнях (пп. 75—81). О модулях, которые являются степенями простых чисел (пп. 82—89). Модули, являющиеся степенями числа 2 (пп. 90, 91). Модули, составленные из нескольких простых чисел (пп. 92, 93). |           |

## Раздел IV. О сравнениях второй степени . . . . . 94

Квадратичные вычеты и невычеты (пп. 94, 95). Если модуль есть простое число, то среди чисел, меньших его, количество вычетов равно количеству невычетов (пп. 96, 97). Ответ на вопрос, является ли составное число вычетом или невычетом заданного простого числа, зависит от свойств сомножителей (пп. 98, 99). О модулях, являющихся составными числами (пп. 100—105). Общий критерий того, является ли заданное число вычетом или невычетом по заданному простому модулю (п. 106). Исследование относительно простых чисел, по которым заданные числа являются вычетами или невычетами (пп. 107—150). Вычет  $-1$  (пп. 108—111). Вычеты  $+2$  и  $-2$  (пп. 112—116). Вычеты  $+3$  и  $-3$  (пп. 117—120). Вычеты  $+5$  и  $-5$  (пп. 121—123). О вычетах  $\pm 7$  (п. 124). Подготовка к общему исследованию (пп. 125—129). Индуктивным путем находится общая (фундаментальная) теорема и делаются выводы из нее (пп. 130—134). Строгое доказательство фундаментальной теоремы (пп. 135—144). Аналогичный метод для доказательства теоремы из п. 114 (п. 145). Решение общей проблемы (п. 146). О линейных формах, содержащих все простые числа, по которым заданное число является вычетом или невычетом (пп. 147—150). О работах других авторов, относящихся к этим исследованиям (п. 151). О сравнениях второй степени общего вида (п. 152).

## Раздел V. О формах и неопределенных уравнениях второй степени . . . . . 151

Предмет исследования; определение форм и обозначения (п. 153). Представление чисел; определитель (п. 154). Значения выражения  $\sqrt{b^2 - ac} \pmod{M}$ , которым принадлежит представление числа  $M$  формой  $(a, b, c)$  (пп. 155, 156). Форма, содержащая другую форму или содержащаяся в другой форме; преобразование, собственное и несобственное (п. 157). Эквивалентность, собственная и несобственная (п. 158). Противоположные формы (п. 159). Соседние формы (п. 160). Общие делители коэффициентов форм (п. 161). Связь между всевозможными однотипными преобразованиями одной заданной формы в другую (п. 162). Двусторонние формы (п. 163). Теорема, касающаяся случая, когда одна форма содержится в другой одновременно собственно и несобственно (пп. 164, 165). Общее исследование о представлениях чисел формами и о связи этих представлений с преобразованиями (пп. 166—170). О формах с отрицательным определителем (пп. 171—182). Специальные приложения к разложению чисел на два квадрата, на простой и удвоенный и на простой и утроенный квадраты (п. 182). О формах с положитель-

н ы м   н е к в а д р а т н ы м   о п р е д е л и т е л е м (пп. 183—205). О   ф о р м а х   с   к в а д р а т н ы м   о п р е д е л и т е л е м (пп. 206—212). Формы, которые содержатся в других, и притом им не эквивалентны (пп. 213, 214). Ф о р м ы   с   о п р е д е л и т е л е м 0 (п. 215). Общее решение в целых числах всех неопределенных уравнений второй степени с двумя неизвестными (пп. 216—221). Исторические замечания (п. 222). Дальнейшие исследования о формах (пп. 223—265). Разбиение форм с заданным определителем на классы (пп. 223—225). Разбиение классов на порядки (пп. 226, 227). Деление порядков на роды (пп. 228—233). О   к о м п о з и ц и и   ф о р м (пп. 234—244). Композиция порядков (п. 245). Композиция родов (пп. 246—248). Композиция классов (пп. 249—251). Для заданного определителя в отдельных родах из одного и того же порядка содержится по одинаковому числу классов (п. 252). Сравниваются количества классов, содержащихся в отдельных родах из различных порядков (пп. 253—256). О числе двусторонних классов (пп. 257—260). Половине всех возможных для данного определителя характеров заведомо не могут соответствовать собственно примитивные (при отрицательном определителе положительные роды) (п. 261). В т о р о е   д о к а з а т е л ь с т в о   ф у н д а м е н т а л ь н о й   т е о р е м ы   и   о с т а л ь н ы х   т е о р е м ,   к а с а ю щ и х с я   в ы ч е т о в  $-1$ ,  $+2$ ,  $-2$  (п. 262). Точнее определяется та половина характеров, которой не могут соответствовать роды (пп. 263, 264). Специальной метод для разложения простых чисел на два квадрата (п. 265). Отступление, содержащее исследование о тройничных формах (пп. 266—285). Некоторые приложения к теории двойничных форм (пп. 286—307). О нахождении формы, при удвоении которой получается заданная двойничная форма главного рода (п. 286). Всем характерам, за исключением тех, невозможность которых была доказана в пп. 263, 264, действительно соответствуют роды (п. 287). Теория разложения чисел и двойничных форм на три квадрата (пп. 288—292). Доказательство теоремы Ф е р м а о том, что каждое целое число может быть разложено на три треугольных числа или на четыре квадрата (п. 293). Решение уравнения  $ax^2 + by^2 + cz^2 = 0$  (пп. 294, 295). О методе, которым Л е ж а н д р изложил фундаментальную теорему (пп. 296—298). Представление нуля любыми тройничными формами (п. 299). Общее решение в рациональных величинах уравнений второй степени с двумя неизвестными (п. 300). О среднем количестве родов (п. 301). О среднем количестве классов (пп. 302—304). Особый алгоритм для собственно примитивных классов; регулярные и иррегулярные определители и т. д. (пп. 305—307).

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>Раздел VI. Различные применения предыдущих исследований</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 468 |
| Разложение дробей на более простые (пп. 309—311). Превращение обыкновенных дробей в десятичные (пп. 312—318). Решение сравнения $x^2 \equiv A$ методом исключения (пп. 319—322). Решение неопределенного уравнения $mx^2 + ny^2 = A$ методом исключения (пп. 323—326). Другой метод решения сравнения $x^2 \equiv A$ в случае, когда $A$ отрицательно (пп. 327, 328). Два метода отличать составные числа от простых и находить сомножители составных чисел (пп. 329—334).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |     |
| <b>Раздел VII. Об уравнениях, от которых зависит деление круга</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 509 |
| Исследование сводится к простейшему случаю, когда число частей, на которые должен быть разбит круг, является простым (п. 336). Уравнения для тригонометрических функций дуг, составляющих одну или несколько частей полной окружности; сведение тригонометрических функций к корням уравнения $x^n - 1 = 0$ (пп. 337, 338). Теория корней уравнения $x^n - 1 = 0$ (в предположении, что $n$ есть простое число). Если отбросить корень 1, то совокупность ( $\Omega$ ) остальных корней содержится в уравнении $X = x^{n-1} + x^{n-2} + \dots + x + 1 = 0$ (пп. 339, 340). Функция $X$ не может быть разложена на сомножители более низких степеней, все коэффициенты у которых рациональны (п. 341). Указывается цель дальнейших исследований (п. 342). Все корни из $\Omega$ разбиваются на некоторые классы (периоды) (п. 343). Различные теоремы о периодах корней из $\Omega$ (пп. 344—351). На предыдущих исследованиях основывается решение уравнения $X = 0$ (пп. 352—354). Дальнейшие исследования о периодах корней. Суммы, у которых количество членов четно, являются вещественными величинами (п. 355). Об уравнении, определяющем разбиение корней из $\Omega$ на два периода (п. 356). Доказательство теоремы, упомянутой в разделе IV (п. 357). Об уравнении для разбиения корней из $\Omega$ на три периода (п. 358). Сведение уравнений, из которых находятся корни $\Omega$ , к чистым уравнениям (пп. 359, 360). Применение предыдущих исследований к тригонометрическим функциям. Метод различать углы, которым соответствуют отдельные корни из ( $\Omega$ ) (п. 361). Тангенсы, котангенсы, секансы и косекансы определяются по синусам и косинусам без помощи деления (п. 362). Метод постепенного понижения степеней уравнений для тригонометрических функций (пп. 363, 364). Деления круга, которые можно выполнить при помощи квадратных уравнений или посредством геометрических построений (пп. 365, 366). |     |

|                             |     |
|-----------------------------|-----|
| <b>Дополнения</b> . . . . . | 574 |
|-----------------------------|-----|

|                          |     |
|--------------------------|-----|
| <b>Таблицы</b> . . . . . | 576 |
|--------------------------|-----|



# ДРУГИЕ СОЧИНЕНИЯ









## НОВОЕ ДОКАЗАТЕЛЬСТВО ОДНОЙ АРИФМЕТИЧЕСКОЙ ТЕОРЕМЫ

*(Commentationes soc. reg; sc. Gottingensis,  
Vol. XVI, Gottingae, 1808)*

### 1

В вопросах высшей арифметики очень часто имеет место своеобразное явление, существенно увеличивающее ее прелесть, которое в анализе встречается значительно реже. В то время как при аналитических исследованиях к новым истинам большей частью можно придти лишь тогда, когда мы полностью овладели принципами, на которых они покоятся, и которые, в известной мере, открывают к ним путь, в арифметике весьма часто, благодаря какому-нибудь неожиданному случаю, бросаются в глаза на индуктивном пути изящнейшие истины, доказательства которых, однако, скрыты так глубоко, что не поддаются никаким попыткам и оказываются недоступными для остроумнейших изысканий. Далее, между арифметическими истинами на первый взгляд совершенно различной природы существует столь тесная и столь поразительная связь, что нередко во время поисков чего-нибудь совсем иного удается на пути, совершенно отличном от ожидаемого, получить какое-нибудь давно желанное доказательство, долгие размышления над которым прежде оставались тщетными. Большой частью, однако, эти истины такого рода, что к ним можно придти многими весьма различными путями, и не всегда кратчайшим оказывается тот, который представился первым. Поэтому, конечно, весьма ценно, когда в конце концов для одной из таких истин, которая долго и безрезультатно обдумывалась и затем

хотя и была доказана, но длинным окольным путем, удастся найти наиболее простое и естественное доказательство.

## 2

Среди вопросов, о которых мы говорили в предыдущем пункте, выдающееся место занимает теорема, содержащая почти всю теорию квадратичных вычетов, которую мы в *«Арифметических исследованиях»* (раздел IV) называли фундаментальной теоремой. Первым, кто нашел эту чрезвычайно изящную теорему, следует, несомненно, считать Л е ж а н д р а, хотя еще задолго до этого великие математики Э й л е р и Л а г р а н ж открыли индуктивным путем многие ее специальные случаи. Я не буду останавливаться здесь на перечислении попыток этих ученых доказать теорему; тот, кого это интересует, может обратиться к упомянутому выше сочинению. Позволю себе лишь, для подтверждения сказанного в предыдущем пункте, добавить здесь то, что относится к моим собственным попыткам. К самой теореме я вполне самостоятельно пришел в 1795 г., когда я еще совершенно не был знаком со всем тем, что было до этого уже сделано в высшей арифметике, и был лишен каких-либо литературных вспомогательных средств; эта теорема мучила меня целый год и не поддавалась напряженнейшим усилиям; наконец, я получил доказательство, приведенное в четвертом разделе указанного сочинения. После этого я нашел еще три других доказательства, основанных на совершенно отличных принципах, одно из которых я сообщил в пятом разделе, а два остальных, которые по изяществу не уступают первому, опубликую при другом удобном случае. Однако все эти доказательства, хотя и не оставляющие желать ничего лучшего в отношении строгости, выведены из слишком разнородных принципов, за исключением, быть может, первого, которое, однако, проводится посредством утомительной цепи умозаключений и страдает чрезмерными длиннотами в вычислениях. Поэтому я, не колеблясь, утверждаю, что естественное доказательство до сих пор отсутствовало; знатоки смогут судить, заслуживает ли такого наименования доказательство, которое нам недавно посчастливилось открыть, и которое излагается на следующих ниже страницах.

## 3

**Теорема.** Пусть  $p$  — положительное простое число,  $k$  — не делящееся на  $p$  целое число,

$A$  — совокупность чисел  $1, 2, 3, \dots, (p-1)/2$ ,

$B$  — совокупность чисел  $(p+1)/2, (p+3)/2, (p+5)/2, \dots, p-1$ .

Возьмем, далее, наименьшие положительные вычеты произведений  $k$  на отдельные числа из  $A$  по модулю  $p$ , которые, очевидно, будут все различны и будут частью принадлежать к  $A$ , а частью к  $B$ . Если теперь предположить, что всего к  $B$  принадлежит  $\mu$  из этих вычетов, то  $k$  будет квадратичным вычетом или невычетом по модулю  $p$  в зависимости от того, будет ли число  $\mu$  четным или нечетным.

**Доказательство.** Если  $a, a', a'', \dots$  суть вычеты, принадлежащие к  $A$ , а  $b, b', b'', \dots$  — остальные вычеты, принадлежащие к  $B$ , то очевидно, что дополнения последних,  $p-b, p-b', p-b'', \dots$ , будут все отличны от чисел  $a, a', a'', \dots$ , но вместе с ними будут исчерпывать всю совокупность  $A$ . Поэтому мы имеем

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{1}{2}(p-1) = aa'a'' \cdot \dots \cdot (p-b)(p-b')(p-b'') \cdot \dots$$

Последнее же произведение, очевидно, будет

$$\begin{aligned} &\equiv (-1)^\mu aa'a'' \cdot \dots \cdot bb'b'' \cdot \dots \equiv \\ &\equiv (-1)^\mu k \cdot 2k \cdot 3k \cdot \dots \cdot \frac{1}{2}(p-1)k \equiv \\ &\equiv (-1)^\mu k^{(p-1)/2} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{1}{2}(p-1) \pmod{p}. \end{aligned}$$

Следовательно,

$$1 \equiv (-1)^\mu k^{(p-1)/2},$$

т. е.  $k^{(p-1)/2} \equiv \pm 1$ , в зависимости от того, будет ли  $\mu$  четным или нечетным, откуда тотчас же и получается наша теорема.

## 4

Дальнейшие рассуждения могут быть существенно сокращены посредством введения подходящих обозначений. Пусть символ  $(k, p)$

обозначает количество тех произведений из ряда

$$k, 2k, 3k, \dots, \frac{1}{2}(p-1)k,$$

наименьшие положительные вычеты которых по модулю  $p$  превосходят половину этого числа. Если далее,  $x$  есть некоторая нецелочисленная величина, то через  $[x]$  мы будем обозначать ближайшее к  $x$ , меньшее чем  $x$  целое число, так что  $x - [x]$  всегда есть положительная величина, лежащая между границами 0 и 1. Тогда без труда получаются следующие соотношения:

I.  $[x] + [-x] = -1.$

II.  $[x] + h = [x + h]$ , если  $h$  есть целое число.

III.  $[x] + [h - x] = h - 1.$

IV. Если  $x - [x]$  есть дробь, меньшая чем  $1/2$ , то  $[2x] - 2[x] = 0$ ; если же, напротив,  $x - [x] > \frac{1}{2}$ , то  $[2x] - 2[x] = 1.$

V. Если поэтому наименьший положительный вычет целого числа  $h$  по модулю  $p$  меньше чем  $p/2$ , то  $[2h/p] - 2[h/p] = 0$ ; если же этот вычет больше чем  $p/2$ , то  $[2h/p] - 2[h/p] = 1.$

VI. Из этого тотчас же следует, что

$$(k, p) = [2k/p] + [4k/p] + [6k/p] + \dots + [(p-1)k/p] - 2[k/p] - 2[2k/p] - 2[3k/p] - \dots - 2\left[\frac{1}{2}(p-1)k/p\right].$$

VII. Из VI и I легко выводится, что

$$(k, p) + (-k, p) = \frac{1}{2}(p-1).$$

Отсюда получается, что число  $-k$  относится к числу  $p$  (в смысле того, является ли  $-k$  вычетом или невычетом по модулю  $p$ ) или так же, как  $+k$ , или противоположным образом, в зависимости от того, имеет ли  $p$  вид  $4n+1$  или вид  $4n+3$ . В первом случае число  $-1$  будет, очевидно, вычетом, а во втором — невычетом по модулю  $p$ .

VIII. Приведенную в VI формулу мы преобразуем следующим образом. Согласно III, имеет место

$$\begin{aligned} [(p-1)k/p] &= k-1-[k/p], \quad [(p-3)k/p] = k-1-[3k/p], \\ [(p-5)k/p] &= k-1-[5k/p], \dots \end{aligned}$$

Если мы произведем замену такими выражениями последних  $(p \mp 1)/4$  членов ряда из VI, то получим,

во-первых, что если  $p$  имеет вид  $4n + 1$ , то

$$(k, p) = \frac{1}{4} (k - 1) (p - 1) - \\ - 2 \left\{ [k/p] + [3k/p] + [5k/p] + \dots + \left[ \frac{1}{2} (p - 3) k / p \right] \right\} - \\ - \left\{ [k/p] + [2k/p] + [3k/p] + \dots + \left[ \frac{1}{2} (p - 1) k / p \right] \right\},$$

и, во-вторых, что если  $p$  имеет вид  $4n + 3$ , то

$$(k, p) = \frac{1}{4} (k - 1) (p + 1) - \\ - 2 \left\{ [k/p] + [3k/p] + [5k/p] + \dots + \left[ \frac{1}{2} (p - 1) k / p \right] \right\} - \\ - \left\{ [k/p] + [2k/p] + [3k/p] + \dots + \left[ \frac{1}{2} (p - 1) k / p \right] \right\}.$$

IX. Для специального случая  $k = +2$  из приведенных выше формул получается, что  $(2, p) = \frac{1}{4} (p \mp 1)$ , где нужно брать верхний или нижний знак в зависимости от того, имеет ли  $p$  вид  $4n + 1$  или  $4n + 3$ . Следовательно, когда  $p$  имеет вид  $8n + 1$  или  $8n + 7$ , число  $(2, p)$  будет четным, и потому 2 будет вычетом по модулю  $p$ ; если же  $p$  имеет вид  $8n + 3$  или  $8n + 5$ , то  $(2, p)$ , напротив, будет нечетным, и потому 2 будет невычетом по модулю  $p$ .

## 5

**Теорема.** Пусть  $x$  — положительная нецелочисленная величина, такая, что среди ее кратностей  $x, 2x, 3x, \dots$  до  $nx$  нет ни одного целого числа; положим  $[nx] = h$ , откуда легко получить, что и среди кратностей  $1/x, 2/x, 3/x, \dots$  до  $h/x$  обратной к  $x$  величины тоже нет целых чисел. Тогда я утверждаю, что

$$[x] + [2x] + [3x] + \dots + [nx] + \\ + [1/x] + [2/x] + [3/x] + \dots + [h/x] = nh.$$

**Доказательство.** В ряде  $[x] + [2x] + [3x] + \dots + [nx]$ , который мы обозначим через  $\Omega$ , первые члены до  $[1/x]$ -го члена включи-

тельно все, очевидно, равны 0, следующие члены до  $[2/x]$ -го все равны 1, следующие, до  $[3/x]$ -го, все равны 2, и т. д. Поэтому

[illegible]

Это и требовалось доказать.

6

**Теорема.** Если  $k, r$  обозначают любые положительные не равные между собой простые числа, то

$$\begin{aligned} & [k/p] + [2k/p] + [3k/p] + \cdots + \left[ \frac{1}{2} (p-1) k/p \right] + \\ & + [p/k] + [2p/k] + [3p/k] + \cdots + \left[ \frac{1}{2} (k-1) p/k \right] = \\ & = \frac{1}{4} (k-1) (p-1). \end{aligned}$$

**Доказательство.** Предположим, для определенности, что  $k < p$ , тогда  $\frac{1}{2}(p-1)k/p$  будет меньше, чем  $k/2$ , но больше чем  $(k-1)/2$  и потому  $\left[\frac{1}{2}(p-1)k/p\right] = \frac{1}{2}(k-1)$ . Отсюда вытекает, что настоящая теорема тотчас же получается из предыдущей, если положить  $\frac{k}{p} = x$ ,  $\frac{1}{2}(p-1) = n$ , и потому  $\frac{1}{2}(k-1) = h$ .

Подобным же образом можно показать, что если  $k$  есть четное число, взаимно простое с  $p$ , то

$$[k/p] + [2k/p] + [3k/p] + \dots + \left[ \frac{1}{2} (p-1) k/p \right] + \\ + [p/k] + [2p/k] + [3p/k] + \dots + \left[ \frac{1}{2} kp/k \right] = \frac{1}{4} k (p-1).$$

Однако мы не будем останавливаться на этой теореме, которая для нашей цели не требуется.

## 7

Теперь из соединения последней теоремы с теоремой VIII п. 4 сразу получается фундаментальная теорема. Именно, если обозначить через  $k$ ,  $p$  какие-нибудь неравные положительные простые числа и положить

$$(k, p) + [k/p] + [2k/p] + [3k/p] + \dots + \left[ \frac{1}{2} (p-1) k/p \right] = L,$$

$$(p, k) + [p/k] + [2p/k] + [3p/k] + \dots + \left[ \frac{1}{2} (k-1) p/k \right] = M,$$

то из VIII п. 4 вытекает, что  $L$  и  $M$  всегда будут четными числами. Согласно же теореме п. 6,

$$L + M = (k, p) + (p, k) + \frac{1}{4} (k-1) (p-1).$$

Поэтому, если  $\frac{1}{4} (k-1) (p-1)$  четно, что будет тогда, когда либо оба числа  $k$ ,  $p$ , либо по крайней мере одно из них имеет вид  $4n+1$ , то  $(k, p)$  и  $(p, k)$  будут обязательно либо оба четны, либо оба нечетны. Если же  $\frac{1}{4} (k-1) (p-1)$  нечетно, что будет тогда, когда оба числа  $k$ ,  $p$  имеют вид  $4n+3$ , то обязательно одно из чисел  $(k, p)$ ,  $(p, k)$  должно быть четным, а другое нечетным. Следовательно, в первом случае отношение числа  $k$  к  $p$  (в том смысле, является ли первое вычетом или невычетом второго) будет совпадать с отношением  $p$  к  $k$ , а во втором случае будет ему противоположно. Это и требовалось доказать.

---



## СУММИРОВАНИЕ НЕКОТОРЫХ РЯДОВ ОСОБОГО ВИДА

(*Commentationes soc. reg. sc. Gotting.  
recentiores, Vol. I, Gottingae, 1811*)

### 1

Среди наиболее замечательных истин, к открытию которых положила путь теория деления круга, далеко не последнее место занимает изложенное в п. 356 «Арифметических исследований» суммирование, причем не только вследствие его особенного изящества и исключительной плодотворности, более подробное обоснование которой мы отложим до другого исследования, но также и по той причине, что строгое и совершенное доказательство этого суммирования требует преодоления совсем необычных трудностей. Эти трудности тем более неожиданны, что относятся они не столько к самой теореме, сколько к некоторому ее уточнению, причем если на него не обращать внимания, то доказательство тотчас же становится очевидным и легко получается на основании изложенной в указанной работе теории. Теорема там была дана в следующем виде. Пусть  $n$  — простое число; обозначим всевозможные квадратичные вычеты по модулю  $n$ , лежащие между границами 0 и  $n - 1$  включительно, через  $a$ , а всевозможные невычеты, лежащие между теми же границами, через  $b$ ; наконец, через  $\omega$  обозначим дугу  $360^\circ/n$ , и через  $k$  — какое-нибудь не делящееся на  $n$  заданное целое число.

I. Тогда для значения  $n$  вида  $4m + 1$  имеет место

$$\sum \cos ak \omega = -\frac{1}{2} \pm \frac{1}{2} \sqrt{n},$$

$$\sum \cos bk \omega = -\frac{1}{2} \mp \sqrt{n},$$

потому

$$\sum \cos ak \omega - \sum \cos bk \omega = \pm \sqrt{n},$$

$$\sum \sin ak \omega = 0,$$

$$\sum \sin bk \omega = 0.$$

II. Для значения  $n$  вида  $4m + 3$  имеет место

$$\sum \cos ak \omega = -\frac{1}{2},$$

$$\sum \cos bk \omega = -\frac{1}{2},$$

$$\sum \sin ak \omega = \pm \frac{1}{2} \sqrt{n},$$

$$\sum \sin bk \omega = \mp \frac{1}{2} \sqrt{n},$$

$$\sum \sin ak \omega - \sum \sin bk \omega = \pm \sqrt{n}.$$

Формулы суммирования были доказаны в упомянутом месте со всей строгостью, и здесь уже не остается больше никаких других трудностей, кроме *определения знака у квадратного корня*. При этом без труда можно показать, что знак зависит от числа  $k$  лишь постольку, поскольку для всех значений  $k$ , которые являются квадратичными вычетами по модулю  $n$ , он должен быть одним и тем же, а для всех значений  $k$ , которые являются квадратичными невычетами по модулю  $n$ , должен быть противоположным первому. Поэтому все дело сводится к случаю  $k=1$ , и ясно, что если мы узнаем знак для этого значения, то он сразу станет известным и для всех остальных значений  $k$ . Но при определении этого знака, которое на первый взгляд кажется относящимся к числу совсем простых задач, мы наталкиваемся на совершенно неожиданные трудности, и метод, при помощи которого мы до сих пор обходили все припятствия, здесь совершенно отказывается служить.

## 2

Быть может целесообразно, прежде чем идти дальше, проделать для нескольких примеров наше суммирование непосредственным вычислением; однако будет хорошо, если предварительно мы сделаем некоторые общие замечания.

I. Если в случае, когда  $n$  есть простое число вида  $4t + 1$ , обозначить через  $a'$  всевозможные квадратичные вычеты по модулю  $n$ , лежащие в границах от 1 до  $(n - 1)/2$  включительно, а через  $b'$  обозначить всевозможные лежащие между теми же границами невычеты, то, как известно, всевозможные числа  $n - a'$  будут содержаться среди чисел  $a$ , а всевозможные числа  $n - b'$  — среди чисел  $b$ ; так как при этом числа  $a', b', n - a', n - b'$  будут, очевидно, составлять всю совокупность чисел  $1, 2, 3, \dots, n - 1$ , то всевозможные  $a'$  вместе со всевозможными  $n - a'$  будут охватывать всевозможные числа  $a$ , и точно так же всевозможные  $b'$  вместе со всевозможными  $n - b'$  будут представлять все числа  $b$ .

Поэтому

$$\begin{aligned}\sum \cos ak\omega &= \sum \cos a'k\omega + \sum \cos (n - a')k\omega, \\ \sum \cos bk\omega &= \sum \cos b'k\omega + \sum \cos (n - b')k\omega, \\ \sum \sin ak\omega &= \sum \sin a'k\omega + \sum \sin (n - a')k\omega, \\ \sum \sin bk\omega &= \sum \sin b'k\omega + \sum \sin (n - b')k\omega.\end{aligned}$$

Но так как  $\cos (n - a')k\omega = \cos a'k\omega$ ,  $\cos (n - b')k\omega = \cos b'k\omega$ ,  $\sin (n - a')k\omega = -\sin a'k\omega$ ,  $\sin (n - b')k\omega = -\sin b'k\omega$ , то сразу очевидно, что имеет место

$$\begin{aligned}\sum \sin ak\omega &= \sum \sin a'k\omega - \sum \sin a'k\omega = 0, \\ \sum \sin bk\omega &= \sum \sin b'k\omega - \sum \sin b'k\omega = 0.\end{aligned}$$

Сумма же косинусов принимает вид

$$\begin{aligned}\sum \cos ak\omega &= 2 \sum \cos a'k\omega, \\ \sum \cos bk\omega &= 2 \sum \cos b'k\omega,\end{aligned}$$

так что должно иметь место

$$1 + 4 \sum \cos a'k\omega = \pm \sqrt{n},$$

$$1 + 4 \sum \cos b'k\omega = \mp \sqrt{n},$$

$$2 \sum \cos a'k\omega - 2 \sum \cos b'k\omega = \pm \sqrt{n}.$$

II. В случае, когда  $n$  имеет вид  $4m + 3$ , дополнение до  $n$  каждого вычета  $a$  является невычетом, а дополнение каждого невычета  $b$  — вычетом; поэтому всевозможные числа  $n - a$  совпадают со всевозможными числами  $b$ , а всевозможные числа  $n - b$  — со всевозможными числами  $a$ . Из этого следует, что

$$\sum \cos ak\omega = \sum \cos (n - b)k\omega = \sum \cos bk\omega.$$

Тем самым, так как всевозможные  $a$  и  $b$  вместе составляют всю совокупность чисел  $1, 2, 3, \dots, n - 1$ , и потому  $\sum \cos ak\omega + \sum \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \dots + \cos (n - 1)k\omega = -1$ , становятся непосредственно очевидными формулы суммирования

$$\sum \cos ak\omega = -\frac{1}{2}, \quad \sum \cos bk\omega = -\frac{1}{2}.$$

Точно так же

$$\sum \sin ak\omega = \sum \sin (n - b)k\omega = -\sum \sin bk\omega,$$

откуда становится ясным, каким образом одна из двух формул суммирования

$$2 \sum \sin ak\omega = \pm \sqrt{n},$$

$$2 \sum \sin bk\omega = \mp \sqrt{n}$$

зависит от другой.

Теперь мы сделаем непосредственные вычисления для нескольких примеров.

I. Для  $n = 5$  имеется одно значение для  $a'$ , именно,  $a' = 1$ , и одно значение для  $b'$ , именно,  $b' = 2$ . Но

$$\cos \omega \approx +0,3090169944, \quad \cos 2\omega \approx -0,8090169944;$$

поэтому  $1 + 4 \cos \omega = +\sqrt{5}$ ,  $1 + 4 \cos 2\omega = -\sqrt{5}$ .

II. Для  $n = 13$  имеется три значения для  $a'$ , именно, 1, 3, 4, и столько же значений для  $b'$ , именно, 2, 5, 6; производя вычисления, находим

|                                                 |                                                 |
|-------------------------------------------------|-------------------------------------------------|
| $\cos \omega \approx +0,8854560257$             | $\cos 2\omega \approx +0,5680647467$            |
| $\cos 3\omega \approx +0,1205366803$            | $\cos 5\omega \approx -0,7485107482$            |
| $\cos 4\omega \approx -0,3546048870$            | $\cos 6\omega \approx -0,9709418174$            |
| <u>Сумма <math>\approx +0,6513878190</math></u> | <u>Сумма <math>\approx -1,1513878189</math></u> |

Поэтому  $1 + 4 \sum \cos a'\omega = +\sqrt{13}$ ,  $1 + 4 \sum \cos b'\omega = -\sqrt{13}$ .

III. Для  $n = 17$  мы имеем четыре значения для  $a'$ , именно, 1, 2, 4, 8, и столько же значений для  $b'$ , именно, 3, 5, 6, 7. Вычисляем теперь косинусы.

|                                                 |                                                 |
|-------------------------------------------------|-------------------------------------------------|
| $\cos \omega \approx +0,9324722294$             | $\cos 3\omega \approx +0,4457383558$            |
| $\cos 2\omega \approx +0,7390089172$            | $\cos 5\omega \approx -0,2736629901$            |
| $\cos 4\omega \approx +0,0922683595$            | $\cos 6\omega \approx -0,6026346364$            |
| $\cos 8\omega \approx -0,9829730997$            | $\cos 7\omega \approx -0,8502171357$            |
| <u>Сумма <math>\approx +0,7807764064</math></u> | <u>Сумма <math>\approx -1,2807764065</math></u> |

Поэтому  $1 + 4 \sum \cos a'\omega = +\sqrt{17}$ ,  $1 + 4 \sum \cos b'\omega = -\sqrt{17}$ .

IV. Для  $n = 3$  имеется одно значение для  $a$ , именно  $a = 1$ , и ему соответствует

$$\sin \omega = +0,8660254038.$$

Поэтому  $2 \sin \omega = +\sqrt{3}$ .

V. Для  $n = 7$  имеется три значения для  $a$ , именно, 1, 2, 4; поэтому мы имеем такие значения синусов:

$$\begin{aligned} \sin \omega &\approx +0,7818314825 \\ \sin 2\omega &\approx +0,9749279122 \\ \sin 4\omega &\approx -0,4338837391 \\ \hline \text{Сумма} &\approx +1,3228756556, \end{aligned}$$

и потому  $2 \sum \sin a\omega = +\sqrt{7}$ .

VI. Для  $n = 11$  значениями  $a$  являются 1, 3, 4, 5, 9, и им соответствуют синусы

$$\begin{aligned}\sin \omega &\approx + 0,5406408175 \\ \sin 3\omega &\approx + 0,9898214419 \\ \sin 4\omega &\approx + 0,7557495744 \\ \sin 5\omega &\approx + 0,2817325568 \\ \sin 9\omega &\approx - 0,9096319954 \\ \hline \text{Сумма} &\approx + 1,6583123952\end{aligned}$$

и потому  $2 \sum \sin a\omega = +\sqrt{11}$ .

VII. Для  $n = 19$  значениями  $a$  являются числа 1, 4, 5, 6, 7, 9, 11, 16, 17, и им соответствуют синусы

$$\begin{aligned}\sin \omega &\approx + 0,3246994692 \\ \sin 4\omega &\approx + 0,9694002659 \\ \sin 5\omega &\approx + 0,9965844930 \\ \sin 6\omega &\approx + 0,9157733267 \\ \sin 7\omega &\approx + 0,7357239107 \\ \sin 9\omega &\approx + 0,1645945903 \\ \sin 11\omega &\approx - 0,4759473930 \\ \sin 16\omega &\approx - 0,8371664783 \\ \sin 17\omega &\approx - 0,6142127127 \\ \hline \text{Сумма} &\approx + 2,1794494718,\end{aligned}$$

и потому  $2 \sum \sin a\omega = +\sqrt{19}$ .

#### 4

Во всех этих примерах знак корня получается положительным, и этот же факт легко установить и для бóльших значений  $n = 23$ ,  $n = 29$  и т. д., вследствие чего уже становится весьма вероятным, что это верно и вообще. Но доказательство этого обстоятельства не может быть получено на основании принципов, изложенных в указанном выше месте; обстоятельство это с полным правом следует признать лежащим гораздо глубже. Цель настоящего сочинения будет состоять в том, чтобы дать строгое доказательство этой в высшей степени изящной теоремы, которое мы безуспешно искали разными способами на протяжении многих лет и в конце концов счастливо

осуществили благодаря своеобразным и довольно тонким рассмотрением; *одновременно мы обобщим теорему*, что не только не повредит ее изяществу, но, скорее, сделает ее еще изящнее. В заключение мы рассмотрим замечательную тесную связь, имеющуюся между этим суммированием и другой в высшей степени важной арифметической теоремой. Мы надеемся, что эти исследования не только будут интересны для математиков сами по себе, но что и методы, при помощи которых нам удалось все это получить и которые могут оказаться полезными и при рассмотрении других вопросов, окажутся достойными их внимания.

## 5

Наше доказательство основывается на рассмотрении своеобразного типа рядов, члены которых зависят от выражений вида

$$\frac{(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \dots (1 - x^{m-\mu+1})}{(1 - x)(1 - x^2)(1 - x^3) \dots (1 - x^\mu)}.$$

Ради краткости мы обозначим такую дробь через  $(m, \mu)$  и сначала сделаем *некоторые общие замечания относительно функций такого вида*.

I. Если  $m$  является целым положительным числом, меньшим чем  $\mu$ , то функция  $(m, \mu)$ , очевидно, равна нулю, так как числитель содержит сомножитель  $(1 - x^0)$ . Для  $m = \mu$  сомножители в числителе будут совпадать с расположенными в обратном порядке сомножителями знаменателя, так что  $(\mu, \mu) = 1$ ; наконец, в случае, когда  $m$  есть целое положительное число, большее чем  $\mu$ , мы имеем формулы

$$(\mu + 1, \mu) = \frac{1 - x^{\mu+1}}{1 - x} = (\mu + 1, 1),$$

$$(\mu + 2, \mu) = \frac{(1 - x^{\mu+2})(1 - x^{\mu+1})}{(1 - x)(1 - x^2)} = (\mu + 2, 2),$$

$$(\mu + 3, \mu) = \frac{(1 - x^{\mu+3})(1 - x^{\mu+2})(1 - x^{\mu+1})}{(1 - x)(1 - x^2)(1 - x^3)} = (\mu + 3, 3),$$

и вообще

$$(m, \mu) = (m, m - \mu).$$

II. Далее, легко устанавливается, что вообще имеет место

$$(m, \mu + 1) = (m - 1, \mu + 1) + x^{m-\mu-1} (m - 1, \mu).$$

Но так как, точно так же, имеет место

$$\begin{aligned} (m - 1, \mu + 1) &= (m - 2, \mu + 1) + x^{m-\mu-2} (m - 2, \mu), \\ (m - 2, \mu + 1) &= (m - 3, \mu + 1) + x^{m-\mu-3} (m - 3, \mu), \\ (m - 3, \mu + 1) &= (m - 4, \mu + 1) + x^{m-\mu-4} (m - 4, \mu), \end{aligned}$$

и т. д.

и этот ряд может быть продолжен до

$$(\mu + 2, \mu + 1) = (\mu + 1, \mu + 1) + x(\mu + 1, \mu) = (\mu, \mu) + x(\mu + 1, \mu),$$

если  $m$  является целым положительным числом, большим чем  $\mu + 1$ , то

$$\begin{aligned} (m, \mu + 1) &= (\mu, \mu) + x(\mu + 1, \mu) + x^2(\mu + 2, \mu) + \\ &+ x^3(\mu + 3, \mu) + \dots + x^{m-\mu-1}(m - 1, \mu). \end{aligned}$$

Отсюда вытекает, что если для какого-нибудь определенного значения числа  $\mu$  каждая функция  $(m, \mu)$ , где  $m$  обозначает целое положительное число, является целой функцией, то должна быть целой и каждая функция  $(m, \mu + 1)$ . Но так как указанное предположение для  $\mu = 1$  выполняется, оно будет справедливо и для  $\mu = 2$ , а потому и для  $\mu = 3$  и т. д., т. е. вообще для любого положительного целочисленного значения  $\mu$  функция  $(m, \mu)$  будет целой функцией, т. е. произведение

$$(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \dots (1 - x^{m-\mu+1})$$

будет делиться на

$$(1 - x)(1 - x^2)(1 - x^3) \dots (1 - x^\mu).$$

## 6

Теперь мы рассмотрим два ряда, которые оба могут привести нас к цели. Первый ряд следующий:

$$1 - \frac{1 - x^m}{1 - x} + \frac{(1 - x^m)(1 - x^{m-1})}{(1 - x)(1 - x^2)} - \frac{(1 - x^m)(1 - x^{m-1})(1 - x^{m-2})}{(1 - x)(1 - x^2)(1 - x^3)} + \dots,$$



или

$$1 - (m, 1) + (m, 2) - (m, 3) + (m, 4) - \dots;$$

мы обозначим его, ради краткости, через  $f(x, m)$ . Прежде всего, непосредственно ясно, что если  $m$  является целым положительным числом, то этот ряд после  $(m + 1)$ -го члена (который равен  $\pm 1$ ) обрывается, и что поэтому сумма в этом случае должна быть конечной целой функцией от  $x$ . Далее, из п. 5, II вытекает, что вообще для любого значения  $m$  имеет место

$$\begin{aligned} 1 &= 1, \\ -(m, 1) &= -(m-1, 1) - x^{m-1}, \\ +(m, 2) &= +(m-1, 2) + x^{m-2}(m-1, 1), \\ -(m, 3) &= -(m-1, 3) - x^{m-3}(m-1, 2) \\ &\text{и т. д.,} \end{aligned}$$

и потому

$$f(x, m) = 1 - x^{m-1} - (1 - x^{m-2})(m-1, 1) + (1 - x^{m-3})(m-1, 2) - \dots - (1 - x^{m-4})(m-1, 3) + \dots,$$

Но очевидно, что

$$\begin{aligned} (1 - x^{m-2})(m-1, 1) &= (1 - x^{m-1})(m-2, 1), \\ (1 - x^{m-3})(m-1, 2) &= (1 - x^{m-1})(m-2, 2), \\ (1 - x^{m-4})(m-1, 3) &= (1 - x^{m-1})(m-2, 3) \\ &\text{и т. д.;} \end{aligned}$$

поэтому мы получаем уравнение

$$[1] \quad f(x, m) = (1 - x^{m-1}) f(x, m-2).$$

## 7

Так как для  $m = 0$  получается  $f(x, m) = 1$ , то согласно только что найденным формулам мы имеем

$$\begin{aligned} f(x, 2) &= 1 - x, \\ f(x, 4) &= (1 - x)(1 - x^3), \\ f(x, 6) &= (1 - x)(1 - x^3)(1 - x^5), \\ f(x, 8) &= (1 - x)(1 - x^3)(1 - x^5)(1 - x^7) \\ &\text{и т. д.,} \end{aligned}$$

т. е. вообще для каждого четного значения числа  $m$

$$[2] \quad f(x, m) = (1 - x)(1 - x^3)(1 - x^5) \dots (1 - x^{m-1}).$$

Наоборот, так как для  $m = 1$  имеет место  $f(x, m) = 0$ , то и

$$f(x, 3) = 0,$$

$$f(x, 5) = 0,$$

$$f(x, 7) = 0$$

и т. д.,

т. е. вообще для каждого нечетного значения числа  $m$

$$f(x, m) = 0.$$

Впрочем, последние формулы могут быть выведены и из того, что в ряде

$$1 - (m, 1) + (m, 2) - (m, 3) + \dots + (m, m-1) - (m, m)$$

последний член уничтожает первый, предпоследний член уничтожает второй и т. д.

## 8

Хотя для нашей цели достаточно ограничиться случаем, когда  $m$  является нечетным положительным целым числом, но вследствие важности вопроса будет не лишним добавить кое-что относительно случаев, когда  $m$  или дробно или отрицательно. Тогда наш ряд, очевидно, уже не будет обрываться, а будет продолжаться до бесконечности, и, кроме того, легко видеть, что он расходится, если придавать  $x$  значения, меньшие чем 1, так что суммирование возможно только для значений  $x$ , которые больше чем 1.

На основании формулы [1] из п. 6 мы имеем

$$f(x, -2) = \frac{1}{1 - \frac{1}{x}},$$

$$f(x, -4) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}},$$

$$f(x, -6) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}}$$

и т. д.,

так что значение функции  $f(x, m)$  и для отрицательного целочисленного значения  $m$  представимо в конечном виде. Для остальных же значений  $m$  мы следующим образом преобразуем функцию  $f(x, m)$  в бесконечное произведение.

Если  $m$  принимает бесконечно большое отрицательное значение, то функция  $f(x, m)$  переходит в

$$1 + \frac{1}{x-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} \cdot \frac{1}{x^3-1} + \dots$$

Следовательно, этот ряд равен бесконечному произведению

$$\frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}} \cdot \frac{1}{1 - \frac{1}{x^7}} \dots$$

Так как, далее, вообще

$$f(x, m) = f(x, m - 2\lambda) \cdot (1 - x^{m-1})(1 - x^{m-3})(1 - x^{m-5}) \dots (1 - x^{m-2\lambda+1}),$$

то будет иметь место

$$\begin{aligned} f(x, m) &= f(x, -\infty) \cdot (1 - x^{m-1})(1 - x^{m-3})(1 - x^{m-5}) \dots = \\ &= \frac{1 - x^{m-1}}{1 - x^{-1}} \cdot \frac{1 - x^{m-3}}{1 - x^{-3}} \cdot \frac{1 - x^{m-5}}{1 - x^{-5}} \cdot \frac{1 - x^{m-7}}{1 - x^{-7}} \dots, \end{aligned}$$

причем эти сомножители будут, очевидно, все больше и больше приближаться к единице.

Специального рассмотрения заслуживает случай  $m = -1$ , когда

$$f(x, -1) = 1 + x^{-1} + x^{-3} + x^{-5} + x^{-7} + \dots$$

Этот ряд равен, следовательно, бесконечному произведению

$$\frac{1 - x^{-2}}{1 - x^{-1}} \cdot \frac{1 - x^{-4}}{1 - x^{-3}} \cdot \frac{1 - x^{-6}}{1 - x^{-5}} \dots,$$

т. е., если вместо  $x$  подставить  $x^{-1}$ , мы будем иметь

$$1 + x + x^3 + x^5 + \dots = \frac{1 - x^2}{1 - x} \cdot \frac{1 - x^4}{1 - x^3} \cdot \frac{1 - x^6}{1 - x^5} \cdot \frac{1 - x^8}{1 - x^7} \dots$$

Это равенство двух довольно замысловатых выражений, к которому мы еще вернемся в другом месте, конечно, в высшей степени замечательно.

## 9

Во-вторых, мы рассмотрим следующий ряд:

$$1 + x^{\frac{1}{2}} \cdot \frac{1-x^m}{1-x} + x \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-x^2)} + x^{\frac{3}{2}} \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-x^2)(1-x^3)} + \dots,$$

или

$$1 + x^{\frac{1}{2}} (m, 1) + x (m, 2) + x^{\frac{3}{2}} (m, 3) + x^2 (m, 4) + \dots,$$

который мы обозначим через  $F(x, m)$ . В этом исследовании мы ограничимся случаем, когда  $m$  является целым положительным числом, так что и этот ряд будет все время обрываться на  $(m+1)$ -м члене, который равен  $x^{\frac{1}{2}m} (m, m)$ . Так как

$$(m, m) = 1, \quad (m, m-1) = (m, 1), \quad (m, m-2) = (m, 2), \dots,$$

то этот ряд может быть представлен также и в виде

$$F(x, m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)} (m, 1) + x^{\frac{1}{2}(m-2)} (m, 2) + x^{\frac{1}{2}(m-3)} (m, 3) + \dots$$

Отсюда следует, что

$$\begin{aligned} \left(1 + x^{\frac{1}{2}m + \frac{1}{2}}\right) F(x, m) &= 1 + x^{\frac{1}{2}} (m, 1) + x (m, 2) + x^{\frac{3}{2}} (m, 3) + \dots \\ &\dots + x^{\frac{1}{2}} x^m + x \cdot x^{m-1} (m, 1) + x^{\frac{3}{2}} x^{m-2} (m, 2) + \dots \end{aligned}$$

Но так как (п. 5, II)

$$\begin{aligned} (m, 1) + x^m &= (m+1, 1), \\ (m, 2) + x^{m-1} (m, 1) &= (m+1, 2), \\ (m, 3) + x^{m-2} (m, 2) &= (m+1, 3) \end{aligned}$$

и т. д.,

то получается, что

$$[3] \quad \left(1 + x^{\frac{1}{2}m + \frac{1}{2}}\right) F(x, m) = F(x, m+1).$$

Но  $F(x, 0) = 1$ ; поэтому

$$\begin{aligned} F(x, 1) &= 1 + x^{\frac{1}{2}}, \\ F(x, 2) &= (1 + x^{\frac{1}{2}})(1 + x), \\ F(x, 3) &= (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}}) \\ &\text{и т. д.}, \end{aligned}$$

или вообще

$$[4] \quad F(x, m) = (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}}) \dots (1 + x^{\frac{1}{2}m}).$$

## 10

После того как мы предпослали эти предварительные исследования, мы ближе займемся нашей задачей. Так как для значения  $n$ , равного простому числу, все квадраты  $1, 4, 9, \dots, \left(\frac{1}{2}(n-1)\right)^2$  не сравнимы между собой по модулю  $n$ , то их наименьшие вычеты по модулю  $n$  будут, очевидно, совпадать с совокупностью всевозможных чисел  $a$ , и потому

$$\begin{aligned} \sum \cos ak\omega &= \cos k\omega + \cos 4k\omega + \cos 9k\omega + \dots + \cos \left(\frac{1}{2}(n-1)\right)^2 k\omega, \\ \sum \sin ak\omega &= \sin k\omega + \sin 4k\omega + \sin 9k\omega + \dots + \sin \left(\frac{1}{2}(n-1)\right)^2 k\omega. \end{aligned}$$

И точно так же, так как эти квадраты  $1, 4, 9, \dots, \left(\frac{1}{2}(n-1)\right)^2$  в обратном порядке сравнимы с квадратами  $\left(\frac{1}{2}(n+1)\right)^2, \left(\frac{1}{2}(n+3)\right)^2, \left(\frac{1}{2}(n+5)\right)^2, \dots, (n-1)^2$ , то

$$\begin{aligned} \sum \cos ak\omega &= \cos \left(\frac{1}{2}(n+1)\right)^2 k\omega + \cos \left(\frac{1}{2}(n+3)\right)^2 k\omega + \dots + \cos (n-1)^2 k\omega, \\ \sum \sin ak\omega &= \sin \left(\frac{1}{2}(n+1)\right)^2 k\omega + \sin \left(\frac{1}{2}(n+3)\right)^2 k\omega + \dots + \sin (n-1)^2 k\omega. \end{aligned}$$

Поэтому, если положить

$$\begin{aligned} T &= 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega + \dots + \cos (n-1)^2 k\omega, \\ U &= \sin k\omega + \sin 4k\omega + \sin 9k\omega + \dots + \sin (n-1)^2 k\omega, \end{aligned}$$

то будет иметь место

$$1 + 2 \sum \cos ak\omega = T,$$

$$2 \sum \sin ak\omega = U.$$

Отсюда вытекает, что указанные в п. 1 суммирования зависят от суммирования рядов  $T$  и  $U$ ; поэтому, несмотря на то, что нам нужны первые суммирования, мы сосредоточим наше исследование на последних, причем рассмотрим их в такой общности, чтобы охватить не только простые значения числа  $n$ , но также и любые составные значения. Число  $k$  мы будем, однако, предполагать взаимно простым с  $n$ , так как к этому случаю легко может быть сведен и случай, когда  $k$  и  $n$  имеют общий делитель.

# 11

Если мы обозначим мнимую величину  $\sqrt{-1}$  через  $i$  и положим

$$\cos k\omega + i \sin k\omega = r,$$

то мы получим  $r^n = 1$ , т. е.  $r$  будет корнем уравнения  $x^n - 1 = 0$ . Легко видеть, что все числа  $k, 2k, 3k, \dots, (n-1)k$  не делятся на  $n$  и не сравнимы одно с другим по модулю  $n$ ; поэтому все степени

$$1, r, r^2, r^3, \dots, r^{n-1}$$

числа  $r$  различны, а каждая из них тоже удовлетворяет уравнению  $x^n - 1 = 0$ . Следовательно, эти степени будут представлять все корни уравнения  $x^n - 1 = 0$ .

Если бы  $k$  имело с  $n$  общий делитель, то эти выводы были бы неверны. Действительно, если бы  $\nu$  было таким общим делителем, то число  $kn/\nu$  делилось бы на  $n$ , а потому была бы равна единице более низкая степень, чем  $r^n$ , а именно,  $r^{n/\nu}$ . Таким образом, в этом случае степени числа  $r$  будут представлять самое большее  $n/\nu$  корней уравнения  $x^n - 1 = 0$ , причем они действительно будут представлять в точности столько различных корней, если  $\nu$  является наибольшим общим делителем чисел  $k$  и  $n$ . В нашем случае, когда  $k$  и  $n$  предполагаются взаимно простыми, число  $r$  удобно называть

собственным корнем уравнения  $x^n - 1 = 0$ ; напротив, в том случае, когда  $k$  и  $n$  имеют (наибольший) общий делитель  $\nu$ , число  $r$  будет называться **несобственным корнем** этого уравнения; очевидно, однако, что тогда  $r$  будет собственным корнем уравнения  $x^{n/\nu} - 1 = 0$ . Простейшим несобственным корнем является единица, а в том случае, когда число  $n$  простое, других несобственных корней вообще нет.

## 12

Если мы положим теперь

$$W = 1 + r + r^4 + r^9 + \dots + r^{(n-1)^2},$$

то, очевидно, будет выполняться равенство  $W = T + iU$ , и  $T$  будет вещественной частью числа  $W$ , в то время как  $U$  будет получаться из мнимой части числа  $W$  отбрасыванием сомножителя  $i$ . Таким образом, вся задача свелась к отысканию суммы  $W$ ; для этой цели можно использовать либо ряд, рассмотренный в п. 6, либо ряд, суммировать который мы научились в п. 9, однако первый менее удобен в случае, если число  $n$  четно. Все же мы надеемся, что читателю будет приятно, если случай, когда  $n$  нечетно, мы исследуем двумя методами.

Итак, мы предположим сначала, что число  $n$  нечетно, что  $r$  обозначает какой-нибудь собственный корень уравнения  $x^n - 1 = 0$ , и что в функцию  $f(x, m)$  подставлены значения  $x = r$  и  $m = n - 1$ . Тогда, очевидно, будут выполняться равенства

$$\begin{aligned} \frac{1 - x^m}{1 - x} &= \frac{1 - r^{-1}}{1 - r} = -r^{-1}, \\ \frac{1 - x^{m-1}}{1 - x^2} &= \frac{1 - r^{-2}}{1 - r^2} = -r^{-2}, \\ \frac{1 - x^{m-2}}{1 - x^3} &= \frac{1 - r^{-3}}{1 - r^3} = -r^{-3} \end{aligned}$$

и т. д.

до

$$\frac{1 - x}{1 - x^m} = \frac{1 - r^{-m}}{1 - r^m} = -r^{-m}.$$

(Не лишне указать, что эти уравнения справедливы лишь постольку, поскольку  $r$  предполагается собственным корнем; действительно, если бы  $r$  было несобственным корнем, то в некоторых из этих дробей одновременно исчезал бы числитель и знаменатель, и потому дроби становились бы неопределенными.)

Отсюда мы выводим следующее уравнение:

$$\begin{aligned} f(r, n-1) &= 1 + r^{-1} + r^{-3} + r^{-5} + \dots + r^{-\frac{1}{2}(n-1)n} = \\ &= (1-r)(1-r^3)(1-r^5)\dots(1-r^{n-2}). \end{aligned}$$

Такое же уравнение будет иметь место, если вместо  $r$  подставить  $r^\lambda$ , где  $\lambda$  обозначает любое число, взаимно простое с  $n$ ; действительно, тогда  $r^\lambda$  также является собственным корнем уравнения  $x^n - 1 = 0$ . Поэтому если вместо  $r$  мы напишем  $r^{n-2}$  или, что то же самое,  $r^{-2}$ , то получим

$$\begin{aligned} 1 + r^2 + r^6 + r^{12} + \dots + r^{(n-1)n} &= \\ &= (1-r^{-2})(1-r^{-6})(1-r^{-10})\dots(1-r^{-2(n-2)}). \end{aligned}$$

Если обе части этого уравнения умножить на

$$r \cdot r^3 \cdot r^5 \dots r^{n-2} = r^{\frac{1}{4}(n-1)^2},$$

то в силу соотношений

$$\begin{aligned} r^{2+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-3)^2}, & r^{(n-1)n+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+1)^2}, \\ r^{6+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-5)^2}, & r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+3)^2}, \\ r^{12+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-7)^2}, & r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+5)^2} \\ && \text{и т. д.} \end{aligned}$$

получится следующее уравнение

$$\begin{aligned} &r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \dots + r + 1 + \\ &+ r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} + \dots + r^{\frac{1}{4}(2n-2)^2} = \\ &= (r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\dots(r^{n-2}-r^{-n+2}), \end{aligned}$$



или, если по иному расположить члены в левой части,

$$[5] \quad 1 + r + r^4 + \dots + r^{(n-1)^2} = \\ = (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \dots (r^{n-2} - r^{-n+2}).$$

### 13

Сомножители в правой части уравнения [5] могут быть представлены и так:

$$\begin{aligned} r - r^{-1} &= - (r^{n-1} - r^{-n+1}), \\ r^3 - r^{-3} &= - (r^{n-3} - r^{-n+3}), \\ r^5 - r^{-5} &= - (r^{n-5} - r^{-n+5}), \end{aligned}$$

до

$$r^{n-2} - r^{-n+2} = - (r^2 - r^{-2}),$$

после чего указанное уравнение принимает вид

$$W = (-1)^{\frac{1}{2}(n-1)} (r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \dots (r^{n-1} - r^{-n+1}).$$

Если это уравнение перемножить с уравнением [5] в его первоначальной форме, то получается

$$W^2 = (-1)^{(n-1)/2} (r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \dots (r^{n-1} - r^{-n+1}),$$

где  $(-1)^{(n-1)/2}$  или равно  $+1$ , или равно  $-1$ , в зависимости от того, имеет ли  $n$  вид  $4\mu + 1$  или вид  $4\mu + 3$ . Отсюда следует, что

$$W^2 = \pm r^{n(n-1)/2} (1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \dots (1 - r^{-2(n-1)}).$$

Но легко видеть, что числа  $r^{-2}, r^{-4}, r^{-6}, \dots, r^{-2n+2}$  представляют все корни уравнения  $x^n - 1 = 0$ , за исключением корня  $x = 1$ , так что для каждого значения  $x$  должно быть справедливым тождественное соотношение

$$\begin{aligned} (x - r^{-2})(x - r^{-4})(x - r^{-6}) \dots (x - r^{-2n+2}) &= \\ &= x^{n-1} + x^{n-2} + x^{n-3} + \dots + x + 1. \end{aligned}$$

Поэтому, если положить  $x = 1$ , мы получим

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \dots (1 - r^{-2n+2}) = n,$$

и так как, очевидно,  $r^{n(n-1)/2} = 1$ , то наше уравнение переходит в следующее:

$$[6] \quad W^2 = \pm n.$$

Таким образом, в случае, когда  $n$  имеет вид  $4\mu + 1$ , будет иметь место

$$W = \pm \sqrt{n}, \text{ и потому } T = \pm \sqrt{n}, U = 0;$$

напротив, в том случае, когда  $n$  имеет вид  $4\mu + 3$ , будет иметь место

$$W = \pm i\sqrt{n}, \text{ и потому } T = 0, U = \pm \sqrt{n}.$$

#### 14

Метод предыдущего пункта позволяет определить только абсолютные значения величин  $T$ ,  $U$ , и остается неизвестным, нужно ли полагать в первом случае  $T$ , а во втором случае  $U$  равными  $+\sqrt{n}$  или  $-\sqrt{n}$ . Однако, по крайней мере для случая  $k = 1$ , это можно следующим образом определить из уравнения [5]. Так как для  $k = 1$  имеет место

$$\begin{aligned} r - r^{-1} &= 2i \sin \omega, \\ r^3 - r^{-3} &= 2i \sin 3\omega, \\ r^5 - r^{-5} &= 2i \sin 5\omega \\ &\text{и т. д.,} \end{aligned}$$

то указанное уравнение преобразуется в

$$W = (2i)^{(n-1)/2} \sin \omega \cdot \sin 3\omega \cdot \sin 5\omega \dots \sin (n-2)\omega.$$

Но в случае, когда  $n$  имеет вид  $4\mu + 1$ , в ряду нечетных чисел

$$1, 3, 5, 7, \dots, \frac{1}{2}(n-3), \frac{1}{2}(n+1), \dots, n-2$$

содержится  $(n-1)/4$  чисел, которые меньше чем  $n/2$ , и им, очевидно, соответствуют положительные синусы; напротив, остальные  $(n-1)/4$  чисел будут больше чем  $n/2$ , и им будут соответствовать отрицательные синусы. Поэтому произведение всех синусов равно произведению положительной величины на множитель  $(-1)^{(n-1)/4}$ ,

и значит  $W$  равно произведению вещественной положительной величины на множитель  $i^{n-1}$ , равный единице (так как  $i^4 = 1$  и  $n - 1$  делится на 4), т. е.  $W$  является вещественной величиной, так что обязательно должно быть

$$W = + \sqrt{n}, \quad T = + \sqrt{n}.$$

А в том случае, когда  $n$  имеет вид  $4\mu + 3$ , в ряду нечетных чисел

$$1, 3, 5, 7, \dots, \frac{1}{2}(n-1), \frac{1}{2}(n+3), \dots, n-2$$

первые  $(n+1)/4$  чисел будут меньше чем  $n/2$ , а остальные  $(n-3)/4$  чисел — больше чем  $n/2$ . Поэтому среди синусов дуг  $\omega, 3\omega, 5\omega, \dots, (n-2)\omega$  будет  $(n-3)/4$  отрицательных, и значит  $W$  будет произведением сомножителя  $i^{(n-1)/2}$ , вещественной положительной величины и сомножителя  $(-1)^{(n-3)/4}$ ; третий сомножитель равен  $i^{(n-3)/2}$ , и вместе с первым он дает  $i^{n-2} = i$ , так как  $i^{n-3} = 1$ . Поэтому обязательно должно быть

$$W = + i\sqrt{n} \text{ и } U = + \sqrt{n}.$$

## 15

Теперь мы покажем, как те же самые выводы могут быть получены при помощи ряда, рассмотренного в п. 9. Если в уравнении [4] мы вместо  $x^{1/2}$  напомним  $-y^{-1}$ , то получим

$$\begin{aligned} [7] \quad & 1 - y^{-1} \frac{1 - y^{-2m}}{1 - y^{-2}} + y^{-2} \frac{(1 - y^{-2m})(1 - y^{-2m+2})}{(1 - y^{-2})(1 - y^{-4})} - \\ & - y^{-3} \frac{(1 - y^{-2m})(1 - y^{-2m+2})(1 - y^{-2m+4})}{(1 - y^{-2})(1 - y^{-4})(1 - y^{-6})} + \dots \text{ до } (m+1)\text{-го члена} = \\ & = (1 - y^{-1})(1 + y^{-2})(1 - y^{-3})(1 + y^{-4}) \dots (1 \pm y^{-m}). \end{aligned}$$

Если теперь взять за  $y$  собственный корень уравнения  $y^n - 1 = 0$ , например,  $r$ , и одновременно положить  $m = n - 1$ , то будут выполняться соотношения

$$\frac{1 - y^{-2m}}{1 - y^{-2}} = \frac{1 - r^2}{1 - r^{-2}} = -r^2,$$

$$\begin{aligned}\frac{1 - y^{-2m+2}}{1 - y^{-4}} &= \frac{1 - r^4}{1 - r^{-4}} = r^4, \\ \frac{1 - y^{-2m+4}}{1 - y^{-6}} &= \frac{1 - r^6}{1 - r^{-6}} = -r^6, \\ &\dots \dots \dots \\ \frac{1 - y^{-2}}{1 - y^{-2m}} &= \frac{1 - r^{2n-2}}{1 - r^{-2n+2}} = -r^{2n-2},\end{aligned}$$

причем нужно отметить, что ни один из знаменателей  $1 - r^{-2}$ ,  $1 - r^{-4}$ , ... не равен 0. Поэтому уравнение [7] принимает следующий вид:

$$\begin{aligned}1 + r + r^4 + r^9 + \dots + r^{(n-1)^2} &= \\ &= (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \dots (1 + r^{-n+1}).\end{aligned}$$

Если в правой части этого уравнения перемножить первый сомножитель с последним, второй с предпоследним и т. д., то мы получим

$$\begin{aligned}(1 - r^{-1})(1 + r^{-n+1}) &= r - r^{-1}, \\ (1 + r^{-2})(1 - r^{-n+2}) &= r^{n-2} - r^{-n+2}, \\ (1 - r^{-3})(1 + r^{-n+3}) &= r^3 - r^{-3}, \\ (1 + r^{-4})(1 - r^{-n+4}) &= r^{n-4} - r^{-n+4} \\ &\text{и т. д.}\end{aligned}$$

Из этих отдельных произведений получается, как легко видеть, произведение

$$(r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \dots (r^{n-4} - r^{-n+4})(r^{n-2} - r^{-n+2}),$$

и потому это последнее выражение равно

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2} = W.$$

Это уравнение тождественно с уравнением [5] п. 12, полученным при помощи первого ряда; остальные выводы могут быть получены из этого уравнения так же, как в пп. 13 и 14.

Теперь мы переходим к случаю, когда  $n$  является четным числом. Если сначала  $n$  имеет вид  $4\mu + 2$ , т. е. не делится на 4, то ясно, что числа  $\frac{1}{4}n^2$ ,  $\left(\frac{1}{2}n + 1\right)^2 - 1$ ,  $\left(\frac{1}{2}n + 2\right)^2 - 4, \dots$ , т. е. вообще числа вида  $\left(\frac{1}{2}n + \lambda\right)^2 - \lambda^2$  при делении на  $n/2$  дают нечетные частные и потому сравнимы с числом  $n/2$  по модулю  $n$ . Отсюда следует, что если  $r$  является собственным корнем уравнения  $x^n - 1 = 0$ , и потому  $r^{n/2} = -1$ , то выполняются равенства

$$\begin{aligned} r^{\left(\frac{1}{2}n\right)^2} &= -1, \\ r^{\left(\frac{1}{2}n+1\right)^2} &= -r, \\ r^{\left(\frac{1}{2}n+2\right)^2} &= -r^4, \\ r^{\left(\frac{1}{2}n+3\right)^2} &= -r^9 \\ &\text{и т. д.} \end{aligned}$$

Следовательно, в ряду

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2}$$

член  $r^{(n/2)^2}$  будет взаимно уничтожаться с первым членом, следующий за  $r^{(n/2)^2}$  член — со вторым членом, и т. д., и потому

$$W = 0, \quad T = 0, \quad U = 0.$$

# 1

Остается еще только случай, когда  $n$  имеет вид  $4\mu$ , т. е. делится на 4. Здесь числа вида  $\left(\frac{1}{2}n + \lambda\right)^2 - \lambda^2$  делятся на  $n$ , и потому

$$r^{\left(\frac{1}{2}n+\lambda\right)^2} = r^{\lambda^2}.$$

Следовательно, в ряду

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2}$$

член  $r^{(n/2)^2}$  равен первому члену, следующий за  $r^{(n/2)^2}$  член — второму члену и т. д., так что

$$W = 2 \left( 1 + r + r^4 + r^9 + \dots + r^{\left(\frac{1}{2}n-1\right)^2} \right).$$

Если мы теперь предположим, что в уравнении [7] п. 15 положено  $m = \frac{1}{2}n - 1$ , а за  $y$  взят собственный корень уравнения  $y^n - 1 = 0$ , например, корень  $r$ , то уравнение, подобно тому, как в п. 15, принимает вид

$$\begin{aligned} 1 + r + r^4 + \dots + r^{\left(\frac{1}{2}n-1\right)^2} &= \\ &= (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \dots (1 - r^{-\frac{1}{2}n+1}), \end{aligned}$$

откуда

$$[8] W = 2 (1 - r^{-1})(1 + r^{-2})(1 - r^{-3})(1 + r^{-4}) \dots (1 - r^{-\frac{1}{2}n+1}).$$

Так как, далее,  $r^{n/2} = -1$ , и потому выполняются равенства

$$1 + r^{-2} = -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2}),$$

$$1 + r^{-4} = -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4}),$$

$$1 + r^{-6} = -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6})$$

и т. д.,

а произведение сомножителей  $-r^{\frac{1}{2}n-2}, -r^{\frac{1}{2}n-4}, -r^{\frac{1}{2}n-6}, \dots$  до  $-r^2$  равно  $(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}n^2 - \frac{1}{4}n}$ , то последнее уравнение может быть записано также и в виде

$$\begin{aligned} W &= 2(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}n^2 - \frac{1}{4}n} (1 - r^{-1})(1 - r^{-2}) \times \\ &\times (1 - r^{-3})(1 - r^{-4}) \dots (1 - r^{-\frac{1}{2}n+1}). \end{aligned}$$

Так как

$$\begin{aligned} 1 - r^{-1} &= -r^{-1} (1 - r^{-n+1}), \\ 1 - r^{-2} &= -r^{-2} (1 - r^{-n+2}), \\ 1 - r^{-3} &= -r^{-3} (1 - r^{-n+3}) \end{aligned}$$

и т. д.,

то

$$\begin{aligned} (1 - r^{-1}) (1 - r^{-2}) (1 - r^{-3}) \dots (1 - r^{-\frac{1}{2}n+1}) &= \\ &= (-1)^{\frac{1}{2}n-1} r^{-\frac{1}{8}n^2 + \frac{1}{4}n} (1 - r^{-\frac{1}{2}n-1}) (1 - r^{-\frac{1}{2}n-2}) \times \\ &\times (1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1}), \end{aligned}$$

и потому

$$\begin{aligned} W &= 2 (-1)^{\frac{3}{4}n-2} r^{-\frac{1}{16}n^2} (1 - r^{-\frac{1}{2}n-1}) (1 - r^{-\frac{1}{2}n-2}) \times \\ &\times (1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1}). \end{aligned}$$

Если перемножить это выражение для  $W$  с ранее найденным и к обеим частям добавить множитель  $1 - r^{-\frac{1}{2}n}$ , то получится

$$\begin{aligned} (1 - r^{-\frac{1}{2}n}) W^2 &= 4 (-1)^{n-3} r^{-\frac{1}{4}n} (1 - r^{-1}) (1 - r^{-2}) \times \\ &\times (1 - r^{-3}) \dots (1 - r^{-n+1}). \end{aligned}$$

Но

$$\begin{aligned} 1 - r^{-\frac{1}{2}n} &= 2, \\ (-1)^{n-3} &= -1, \\ r^{-\frac{1}{4}n} &= -r^{\frac{1}{4}n} \end{aligned}$$

$$(1 - r^{-1}) (1 - r^{-2}) (1 - r^{-3}) \dots (1 - r^{-n+1}) = n.$$

Из этого следует, наконец, что

$$[9] \quad W^2 = 2r^{n/4} n.$$

Но легко видеть, что  $r^{n/4}$  равно или  $+i$ , или  $-i$ , в зависимости от того, имеет ли  $k$  вид  $4\mu + 1$  или  $4\mu + 3$ . А так как

$$2i = (1 + i)^2, \quad -2i = (1 - i)^2,$$

то в случае, когда  $k$  имеет вид  $4\mu + 1$ , будет иметь место

$$W = \pm (1 + i) \sqrt{n}, \text{ и потому } T = U = \pm \sqrt{n},$$

а в случае, когда  $k$  имеет вид  $4\mu + 3$ , получается

$$W = \pm (1 - i) \sqrt{n}, \text{ и потому } T = -U = \pm \sqrt{n}.$$

## 18

Метод предыдущего пункта позволяет определить абсолютные значения функций  $T$ ,  $U$  и дает условия, при которых они имеют или одинаковые, или противоположные знаки, но не дает еще возможности определить сами знаки. Для случая, когда принято  $k = 1$ , мы завершим это следующим образом.

Если положить  $\rho = \cos \frac{1}{2} \omega + i \sin \frac{1}{2} \omega$ , так что  $r = \rho^2$ , то, в силу равенства  $\rho^n = -1$ , уравнение [8], очевидно, можно будет представить следующим образом:

$$W = 2 (1 + \rho^{n-2}) (1 + \rho^{-4}) (1 + \rho^{n-6}) (1 + \rho^{-8}) \dots (1 + \rho^{-n+4}) (1 + \rho^2),$$

или, если расположить сомножители в другом порядке,

$$W = 2 (1 + \rho^2) (1 + \rho^{-4}) (1 + \rho^6) (1 + \rho^{-8}) \dots (1 + \rho^{-n+4}) (1 + \rho^{n-2}).$$

Но

$$1 + \rho^2 = 2\rho \cos \frac{1}{2} \omega,$$

$$1 + \rho^{-4} = 2\rho^{-2} \cos \omega,$$

$$1 + \rho^6 = 2\rho^3 \cos \frac{3}{2} \omega,$$

$$1 + \rho^{-8} = 2\rho^{-4} \cos 2\omega$$

и т. д.

до

$$1 + \rho^{-n+4} = 2\rho^{-\frac{1}{2}n+2} \cos \left( \frac{1}{4}n - 1 \right) \omega,$$

$$1 + \rho^{n-2} = 2\rho^{\frac{1}{2}n-1} \cos \left( \frac{1}{4}n - \frac{1}{2} \right) \omega.$$



Поэтому мы получаем

$$W = 2^{n/2} \rho^{n/4} \cos \frac{1}{2} \omega \cdot \cos \omega \cdot \cos \frac{3}{2} \omega \dots \cos \left( \frac{1}{4} n - \frac{1}{2} \right) \omega.$$

Входящие в это произведение косинусы, очевидно, все положительные, сомножитель же  $\rho^{n/4}$  равен  $\cos 45^\circ + i \sin 45^\circ = (1 + i) \sqrt{1/2}$ . Отсюда следует, что  $W$  является произведением числа  $(1 + i)$  на вещественную положительную величину, вследствие чего обязательно должно быть

$$W = (1 + i) \sqrt{n} \quad \text{и} \quad = + \sqrt{n}, \quad U = + \sqrt{n}.$$

19

Имеет смысл еще раз сопоставить здесь между собой все произведенные до сих пор суммирования. Именно, вообще имеет место

| $T =$          | $U =$          | В зависимости от того,<br>имеет ли $n$ вид |
|----------------|----------------|--------------------------------------------|
| $\pm \sqrt{n}$ | $\pm \sqrt{n}$ | $4\mu$                                     |
| $\pm \sqrt{n}$ | 0              | $4\mu + 1$                                 |
| 0              | 0              | $4\mu + 2$                                 |
| 0              | $\pm \sqrt{n}$ | $4\mu + 3$                                 |

и в случае, когда предполагается, что  $k = 1$ , корни должны браться с положительными знаками. Поэтому то, что для простых значений числа  $n$  мы нашли в п. 3 индуктивным путем, теперь доказано со всей строгостью, и остается еще только показать, как могут быть во всех случаях определены знаки для любых значений числа  $k$ . Однако, прежде чем мы сможем взяться за эту задачу во всей ее общности, мы должны сначала подробнее рассмотреть те случаи, когда  $n$  является простым числом или степенью простого числа.

Если сначала  $n$  — нечетное простое число, то после изложенного в п. 10 очевидно, что  $W = 1 + 2 \sum r^a = 1 + 2 \sum R^{ak}$ , где  $R = \cos \omega + i \sin \omega$ , и  $a$ , как и там, пробегает все квадратичные вычеты по модулю  $n$  от 1 до  $n-1$ . Если теперь точно так же обозначить через  $b$  всевозможные квадратичные невычеты по модулю  $n$ , лежащие в тех же границах, то легко видеть, что всевозможные числа  $ak$  будут сравнимы по модулю  $n$  (с точностью до порядка расположения) либо со всевозможными числами  $a$ , либо со всевозможными числами  $b$ , в зависимости от того, является ли  $k$  вычетом или невычетом. Поэтому в первом случае

$$W = 1 + 2 \sum R^a = 1 + R + R^4 + R^9 + \dots + R^{(n-1)^2},$$

и потому  $W = +\sqrt{n}$ , если  $n$  имеет вид  $4\mu + 1$ , и  $W = +i\sqrt{n}$ , если  $n$  имеет вид  $4\mu + 3$ .

Во втором случае, когда  $k$  есть невычет по модулю  $n$ , получается

$$W = 1 + 2 \sum R^b.$$

Так как всевозможные числа  $a$ ,  $b$ , очевидно, исчерпывают всю совокупность чисел  $1, 2, 3, \dots, n-1$ , и потому

$$\sum R^a + \sum R^b = R + R^2 + R^3 + \dots + R^{n-1} = -1,$$

то отсюда вытекает, что

$$W = -1 - 2 \sum R^a = -(1 + R + R^4 + R^9 + \dots + R^{(n-1)^2}),$$

и потому  $W = -\sqrt{n}$ , если  $n$  имеет вид  $4\mu + 1$ , и  $W = -i\sqrt{n}$ , если  $n$  имеет вид  $4\mu + 3$ .

Таким образом,

во-первых, если  $n$  имеет вид  $4\mu + 1$  и  $k$  является квадратичным вычетом по модулю  $n$ , то

$$T = +\sqrt{n}, \quad U = 0;$$

во-вторых, если  $n$  имеет вид  $4\mu + 1$ , и  $k$  является квадратичным невычетом по модулю  $n$ , то

$$T = -\sqrt{n}, \quad U = 0,$$

в-третьих, если  $n$  имеет вид  $4\mu + 3$ , и  $k$  является квадратичным вычетом по модулю  $n$ , то

$$T = 0, \quad U = +\sqrt{n};$$

в-четвертых, если  $n$  имеет вид  $4\mu + 3$ , и  $k$  является квадратичным невычетом по модулю  $n$ , то

$$T = 0, \quad U = -\sqrt{n}.$$

## 21

Пусть, во-вторых,  $n$  является или квадратом, или более высокой степенью нечетного простого числа  $p$ , и пусть  $n = p^{2x}q$ , где  $q$  или равно 1, или равно  $p$ . Здесь мы хотим прежде всего заметить, что если  $\lambda$  — какое-нибудь целое число, не делящееся на  $p^x$ , то

$$\begin{aligned} & r^{\lambda^2} + r^{(\lambda+p^xq)^2} + r^{(\lambda+2p^xq)^2} + r^{(\lambda+3p^xq)^2} + \dots + r^{(\lambda+n-p^xq)^2} = \\ & = r^{\lambda^2} (1 + r^{2\lambda p^xq} + r^{4\lambda p^xq} + r^{6\lambda p^xq} + \dots + r^{2\lambda(n-p^xq)}) = \\ & = r^{\lambda^2} \cdot \frac{1 - r^{2\lambda n}}{1 - r^{2\lambda p^xq}} = 0. \end{aligned}$$

Из этого легко видно, что

$$W = 1 + r^{p^{2x}} + r^{4p^{2x}} + r^{9p^{2x}} + \dots + r^{(n-1)2p^{2x}}.$$

Действительно, остальные члены ряда

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2}$$

могут быть разбиты на  $(p^x - 1)q$  частичных рядов, каждый из которых содержит  $p^x$  членов и на основании указанного выше преобразования имеет нулевую сумму.

Отсюда мы заключаем, что в случае, когда  $q = 1$ , т. е.  $n$  является степенью простого числа с четным показателем, выполняется равенство

$$W = p^x = +\sqrt[n]{n}, \text{ и потому } T = +\sqrt[n]{n}, U = 0.$$

В случае же, когда  $q = p$ , т. е. когда  $n$  является степенью простого числа с нечетным показателем, мы положим  $r^{p^{2x}} = \rho$ ; тогда  $\rho$  будет собственным корнем уравнения  $x^p - 1 = 0$ , а именно,  $\rho = \cos \frac{k}{p} 360^\circ + i \sin \frac{k}{p} 360^\circ$ , и

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(p^x+1-1)^2} = \\ &= \rho^x (1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(p-1)^2}). \end{aligned}$$

Но сумма ряда  $1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(p-1)^2}$  определяется так же, как в предыдущем пункте, и мы немедленно получаем, что

$$W = \pm \sqrt[n]{n} = T, \text{ если } p \text{ имеет вид } 4\mu + 1,$$

$$W = \pm i \sqrt[n]{n} = iU, \text{ если } p \text{ имеет вид } 4\mu + 3,$$

причем следует брать положительный или отрицательный знак в зависимости от того, является ли число  $k$  вычетом или невычетом по модулю  $p$ .

## 22

Из того, что было изложено в пп. 20 и 21, легко выводится также следующая теорема, которая позднее будет нам очень полезна. Если положить

$$W' = 1 + r^h + r^{4h} + r^{9h} + \dots + r^{h(n-1)^2},$$

где  $h$  обозначает какое-нибудь не делящееся на  $p$  целое число, то в случае, когда  $n$  или равно  $p$ , или равно степени числа  $p$  с нечетным показателем, имеет место

$$W' = W, \text{ если } h \text{ есть квадратичный вычет по модулю } p,$$

$$W' = -W, \text{ если } h \text{ есть квадратичный невычет по модулю } p.$$

Действительно,  $W'$ , очевидно, получается из  $W$ , если подставить  $kh$  вместо  $k$ ; но в первом случае  $k$  и  $kh$  однотипны, а во втором — неоднотипны, если рассматривать их в отношении свойства быть вычетами или невычетами по модулю  $p$ .

Напротив, в том случае, когда  $n$  является степенью числа  $p$  с четным показателем, очевидно, выполняется равенство  $W' = +\sqrt{n}$ , и потому всегда  $W' = W$ .

## 23

В пп. 20, 21 и 22 мы рассмотрели нечетные простые числа и их степени; поэтому *остается* еще только *случай, когда  $n$  является степенью числа 2*.

Для  $n = 2$ , очевидно,  $W = 1 + r = 0$ .

Для  $n = 4$  получается  $W = 1 + r + r^4 + r^9 = 2 + 2r$ , поэтому  $W = 2 + 2i$ , если  $k$  имеет вид  $4\mu + 1$ , и  $W = 2 - 2i$ , если  $k$  имеет вид  $4\mu + 3$ .

Для  $n = 8$  мы имеем  $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$ . Поэтому

$$W = (1 + i)\sqrt{8}, \text{ если } k \text{ имеет вид } 8\mu + 1,$$

$$W = (-1 + i)\sqrt{8}, \text{ если } k \text{ имеет вид } 8\mu + 3,$$

$$W = (-1 - i)\sqrt{8}, \text{ если } k \text{ имеет вид } 8\mu + 5,$$

$$W = (1 - i)\sqrt{8}, \text{ если } k \text{ имеет вид } 8\mu + 7.$$

Если  $n$  является более высокой степенью числа 2, то мы положим  $n = 2^{2x}q$ , где  $q$  или равно 1, или равно 2, а  $x$  больше чем 1. Здесь прежде всего надо заметить, что если  $\lambda$  есть какое-нибудь не делящееся на  $2^{x-1}$  целое число, то

$$\begin{aligned} & r^{\lambda^2} + r^{(\lambda+2^x q)^2} + r^{(\lambda+2 \cdot 2^x q)^2} + r^{(\lambda+3 \cdot 2^x q)^2} + \dots + r^{(\lambda+n-2^x q)^2} = \\ & = r^{\lambda^2} (1 + r^{2^{x+1}\lambda q} + r^{2 \cdot 2^{x+1}\lambda q} + r^{3 \cdot 2^{x+1}\lambda q} + \dots + r^{(2n-2^{x+1}q)\lambda} = \\ & = r^{\lambda^2} \frac{1 - r^{2\lambda n}}{1 - r^{2^{x+1}\lambda q}} = 0. \end{aligned}$$

Отсюда легко видеть, что

$$W = 1 + r^{2^{2x-2}} + r^{4 \cdot 2^{2x-2}} + r^{9 \cdot 2^{2x-2}} + \dots + r^{(n-2^{x-1})^2}.$$

Если мы положим  $r^{2^{2x-2}} = \rho$ , то  $\rho$  будет корнем уравнения  $x^{4q} - 1 = 0$ , а именно,  $\rho = \cos \frac{k}{4q} 360^\circ + i \sin \frac{k}{4q} 360^\circ$ . Тогда

$$W = 1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(2^{x+1}q-1)^2} = \\ = 2^{x-1} (1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(4q-1)^2}).$$

Но сумма ряда  $1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(4q-1)^2}$  определяется на основании того, что говорилось относительно случаев  $n = 4$ ,  $n = 8$ ; поэтому в случае, когда  $q = 1$ , т. е. когда  $n$  есть степень числа 4, получается, что

$$W = (1 + i)2^x = (1 + i)\sqrt{n}, \text{ если } k \text{ имеет вид } 4\mu + 1,$$

$$W = (1 - i)2^x = (1 - i)\sqrt{n}, \text{ если } k \text{ имеет вид } 4\mu + 3,$$

т. е. получаются формулы, которые в точности аналогичны формулам для случая  $n = 4$ ; если же  $q = 2$ , т. е.  $n$  является степенью числа 2 с нечетным показателем, большим чем 3, то

$$W = (1 + i)2^x\sqrt{2} = (1 + i)\sqrt{n}, \text{ если } k \text{ имеет вид } 8\mu + 1,$$

$$W = (-1 + i)2^x\sqrt{2} = (-1 + i)\sqrt{n}, \text{ если } k \text{ имеет вид } 8\mu + 3,$$

$$W = (-1 - i)2^x\sqrt{2} = (-1 - i)\sqrt{n}, \text{ если } k \text{ имеет вид } 8\mu + 5,$$

$$W = (1 - i)2^x\sqrt{2} = (1 - i)\sqrt{n}, \text{ если } k \text{ имеет вид } 8\mu + 7;$$

эти формулы также совершенно аналогичны тем, которые были указаны для  $n = 8$ .

## 24

Также и здесь есть смысл потрудиться над тем, чтобы определить, как связаны между собой сумма ряда

$$W' = 1 + r^h + r^{4h} + r^{9h} + \dots + r^{h(n-1)^2},$$

где  $h$  обозначает какое-нибудь нечетное число, и сумма  $W$ . Так как  $W'$  получается из  $W$ , если  $k$  заменить на  $kh$ , то значение  $W'$  будет так же зависеть от вида числа  $kh$ , как  $W$  зависит от вида

числа  $k$ . Если положить  $\frac{W'}{W} = l$ , то, очевидно, будет справедливо следующее.

I. В случае, когда  $n = 4$  или когда  $n$  есть более высокая степень числа 2 с четным показателем, имеет место

$$l = 1, \text{ если } h \text{ имеет вид } 4\mu + 1,$$

$$l = -i, \text{ если } h \text{ имеет вид } 4\mu + 3, \text{ а } k \text{ — вид } 4\mu + 1,$$

$$l = +i, \text{ если } h \text{ имеет вид } 4\mu + 3, \text{ и } k \text{ имеет такой же вид.}$$

II. В случае, когда  $n = 8$  или когда  $n$  есть более высокая степень числа 2 с нечетным показателем, имеет место

$$l = 1, \text{ если } h \text{ имеет вид } 8\mu + 1,$$

$$l = -1, \text{ если } h \text{ имеет вид } 8\mu + 5,$$

$$l = +i, \text{ если либо } h \text{ имеет вид } 8\mu + 3, \text{ а } k \text{ — вид } 4\mu + 1,$$

$$\text{либо } h \text{ имеет вид } 8\mu + 7, \text{ а } k \text{ — вид } 4\mu + 3,$$

$$l = -i, \text{ если либо } h \text{ имеет вид } 8\mu + 3, \text{ а } k \text{ — вид } 4\mu + 3,$$

$$\text{либо } h \text{ имеет вид } 8\mu + 7, \text{ а } k \text{ — вид } 4\mu + 1.$$

Изложенным до сих пор полностью завершается определение суммы  $W$  в тех случаях, когда  $n$  является простым числом или степенью простого числа; поэтому остается только исследовать те случаи, когда  $n$  составлено из нескольких простых чисел. К этому нам пролагает путь следующая теорема.

## 25

**Теорема.** Если  $n$  есть произведение двух целых положительных взаимно простых чисел  $a$  и  $b$ , и если

$$P = 1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \dots + r^{(b-1)^2 a^2},$$

$$Q = 1 + r^{b^2} + r^{4b^2} + r^{9b^2} + \dots + r^{(a-1)^2 b^2},$$

то я утверждаю, что  $W = PQ$ .

**Доказательство.** Если число  $\alpha$  пробегает все значения  $0, 1, 2, 3, \dots, a-1$ , число  $\beta$  — все значения  $0, 1, 2, 3, \dots, b-1$ , число  $\nu$  — все значения  $0, 1, 2, 3, \dots, n-1$ , то, очевидно,

$$P = \sum r^{a^2 \beta^2}, \quad Q = \sum r^{b^2 \alpha^2}, \quad W = \sum r^{\nu^2}.$$

Поэтому  $PQ = \sum r^{a^2\beta^2 + b^2\alpha^2}$ , если для  $\alpha$  и  $\beta$  брать всевозможные значения во всевозможных сочетаниях; далее, в силу того, что  $2ab\alpha\beta = 2\alpha\beta n$ , выполняется равенство  $PQ = \sum r^{(a\beta + b\alpha)^2}$ . Но без труда видно, что отдельные значения выражения  $a\beta + b\alpha$  различны между собой, и каждое из них равно какому-нибудь значению  $\gamma$ . Поэтому  $PQ = \sum r^{\gamma^2} = W$ .

Заметим, между прочим, что  $r^{a^2}$  является собственным корнем уравнения  $x^b - 1 = 0$ , а  $r^{b^2}$  — собственным корнем уравнения  $x^a - 1 = 0$ .

## 26

Если, далее,  $n$  является произведением трех попарно взаимно простых чисел  $a$ ,  $b$ ,  $c$ , то очевидно, что если положить  $bc = b'$ , числа  $a$  и  $b'$  также будут взаимно простыми; поэтому  $W$  является произведением двух сомножителей

$$\begin{aligned} &1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \dots + r^{(b'-1)^2 a^2}, \\ &1 + r^{b'^2} + r^{4b'^2} + r^{9b'^2} + \dots + r^{(a-1)^2 b'^2}. \end{aligned}$$

Но так как  $r^{a^2}$  есть собственный корень уравнения  $x^{bc} - 1 = 0$ , то первый сомножитель сам есть произведение сомножителей

$$\begin{aligned} &1 + \rho^{b^2} + \rho^{4b^2} + \rho^{9b^2} + \dots + \rho^{(c-1)^2 b^2}, \\ &1 + \rho^{c^2} + \rho^{4c^2} + \rho^{9c^2} + \dots + \rho^{(b-1)^2 c^2}, \end{aligned}$$

где  $\rho = r^{a^2}$ . Отсюда вытекает, что  $W$  является произведением трех сомножителей

$$\begin{aligned} &1 + r^{b^2 c^2} + r^{4b^2 c^2} + r^{9b^2 c^2} + \dots + r^{(a-1)^2 b^2 c^2}, \\ &1 + r^{a^2 c^2} + r^{4a^2 c^2} + r^{9a^2 c^2} + \dots + r^{(b-1)^2 a^2 c^2}, \\ &1 + r^{a^2 b^2} + r^{4a^2 b^2} + r^{9a^2 b^2} + \dots + r^{(c-1)^2 a^2 b^2}, \end{aligned}$$

где  $r^{b^2 c^2}$ ,  $r^{a^2 c^2}$ ,  $r^{a^2 b^2}$  обозначают соответственно собственные корни уравнений  $x^a - 1 = 0$ ,  $x^b - 1 = 0$ ,  $x^c - 1 = 0$ .



Из этого мы без труда заключаем, что, вообще, если  $n$  есть произведение любого числа попарно взаимно простых сомножителей  $a, b, c, \dots$ , то  $W$  есть произведение такого же числа сомножителей, причем этими последними являются выражения

$$\begin{aligned} &1 + r^{\frac{n^2}{a^2}} + r^{\frac{4n^2}{a^2}} + r^{\frac{9n^2}{a^2}} + \dots + r^{\frac{(a-1)^2n^2}{a^2}}, \\ &1 + r^{\frac{n^2}{b^2}} + r^{\frac{4n^2}{b^2}} + r^{\frac{9n^2}{b^2}} + \dots + r^{\frac{(b-1)^2n^2}{b^2}}, \\ &1 + r^{\frac{n^2}{c^2}} + r^{\frac{4n^2}{c^2}} + r^{\frac{9n^2}{c^2}} + \dots + r^{\frac{(c-1)^2n^2}{c^2}}, \\ &\dots \dots \dots \end{aligned}$$

где  $r^{n^2/a^2}, r^{n^2/b^2}, r^{n^2/c^2} \dots$  являются соответственно собственными корнями уравнений  $x^a - 1 = 0, x^b - 1 = 0, x^c - 1 = 0, \dots$

На основании этих принципов переход к полному определению суммы  $W$  для любого значения числа  $n$  уже ясен. Именно, нужно разложить  $n$  на сомножители  $a, b, c, \dots$ , являющиеся или различными простыми числами, или степенями различных простых чисел, и положить  $r^{n^2/a^2} = A, r^{n^2/b^2} = B, r^{n^2/c^2} = C, \dots$ . Тогда  $A, B, C, \dots$  будут собственными корнями уравнений  $x^a - 1 = 0, x^b - 1 = 0, x^c - 1 = 0, \dots$ , а  $W$  будет произведением сомножителей

$$\begin{aligned} &1 + A + A^4 + A^9 + \dots + A^{(a-1)^2}. \\ &1 + B + B^4 + B^9 + \dots + B^{(b-1)^2}, \\ &1 + C + C^4 + C^9 + \dots + C^{(c-1)^2} \\ &\text{и т. д.} \end{aligned}$$

Но каждый из этих сомножителей может быть определен на основании изложенного в пп. 20, 21 и 23, так что тем самым будет известно и значение произведения. Будет не бесполезным собрать здесь вместе правила для определения указанных сомножителей, что-

бы иметь их одновременно перед собой. Так как корень  $A$  равен  $\frac{kn}{a} \cdot \frac{360^\circ}{a}$ , то сумма  $1 + A + A^4 + A^9 + \dots + A^{(a-1)^2}$ , которую мы обозначим через  $L$ , будет так же определяться числом  $kn/a$ , как в нашем общем исследовании сумма  $W$  определялась числом  $k$ . Нам нужно различать теперь двенадцать случаев.

I. Если  $a$  равно или простому числу  $p$  вида  $4\mu + 1$ , или его степени с нечетным показателем, и одновременно  $kn/a$  является квадратичным вычетом по модулю  $p$ , то  $L = +\sqrt{a}$ .

II. Если при тех же остальных предположениях  $kn/a$  является квадратичным невычетом по модулю  $p$ , то  $L = -\sqrt{a}$ .

III. Если  $a$  равно или простому числу  $p$  вида  $4\mu + 3$ , или его степени с нечетным показателем, и одновременно  $kn/a$  является квадратичным вычетом по модулю  $p$ , то  $L = +i\sqrt{a}$ .

IV. Если при тех же, что и в III, остальных предположениях  $kn/a$  является квадратичным невычетом по модулю  $p$ , то  $L = -i\sqrt{a}$ .

V. Если  $a$  является квадратом или более высокой степенью с четным показателем (нечетного) простого числа, то  $L = +\sqrt{a}$ .

VI. Если  $a = 2$ , то  $L = 0$ .

VII. Если  $a = 4$  или  $a$  является более высокой степенью числа 2 с четным показателем, и одновременно  $kn/a$  имеет вид  $4\mu + 1$ , то  $L = (1 + i)\sqrt{a}$ .

VIII. Если при тех же, что и в VII, остальных предположениях  $kn/a$  имеет вид  $4\mu + 3$ , то  $L = (1 - i)\sqrt{a}$ .

IX. Если  $a = 8$  или  $a$  является более высокой степенью числа 2 с нечетным показателем, и одновременно  $kn/a$  имеет вид  $8\mu + 1$ , то  $L = (1 + i)\sqrt{a}$ .

X. Если при тех же, что и в IX, остальных предположениях  $kn/a$  имеет вид  $8\mu + 3$ , то  $L = (-1 + i)\sqrt{a}$ .

XI. Если при тех же остальных предположениях  $kn/a$  имеет вид  $8\mu + 5$ , то  $L = (-1 - i)\sqrt{a}$ .

XII. Если при тех же остальных предположениях число  $kn/a$  имеет вид  $8\mu + 7$ , то  $L = (1 - i)\sqrt{a}$ .

Пусть, например,  $n = 2520 = 8 \cdot 9 \cdot 5 \cdot 7$  и  $k = 13$ . Тогда  
для  $a = 8$ , согласно случаю XII,  $L = (1 - i)\sqrt{8}$ ;  
для сомножителя 9, согласно случаю V, соответствующая сумма равна  $\sqrt{9}$ ;  
для сомножителя 5, согласно случаю II, соответствующая сумма равна  $-\sqrt{5}$ ;  
для сомножителя 7, согласно случаю III, соответствующая сумма равна  $+i\sqrt{7}$ . Поэтому мы получаем:

$$W = (1 - i)(-i)\sqrt{2520} = (-1 - i)\sqrt{2520}.$$

Если  $n$  имеет это же значение, а  $k = 1$ , то  
сомножителю 8 соответствует сумма  $(-1 + i)\sqrt{8}$ ,  
сомножителю 9 соответствует сумма  $\sqrt{9}$ ,  
сомножителю 5 соответствует сумма  $\sqrt{5}$ ,  
сомножителю 7 соответствует сумма  $-i\sqrt{7}$ .  
Поэтому для произведения получается  $W = (1 + i)\sqrt{2520}$ .

Другой метод для определения суммы  $W$  в общем случае основывается на том, что мы изложили в пп. 22 и 24. Если мы положим вообще  $\cos \omega + i \sin \omega = \rho$  и

$$\rho^{n^2/a^2} = \alpha, \rho^{n^2/b^2} = \beta, \rho^{n^2/c^2} = \gamma, \dots,$$

так что  $r = \rho^k, A = \alpha^k, B = \beta^k, C = \gamma^k, \dots$ , то выражение

$$1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(n-1)^2}$$

будет произведением сомножителей

$$\begin{aligned} &1 + \alpha + \alpha^4 + \alpha^9 + \dots + \alpha^{(a-1)^2}, \\ &1 + \beta + \beta^4 + \beta^9 + \dots + \beta^{(b-1)^2}, \\ &1 + \gamma + \gamma^4 + \gamma^9 + \dots + \gamma^{(c-1)^2}, \\ &\dots \end{aligned}$$

а потому  $W$  будет произведением сомножителей

$$\begin{aligned} w &= 1 + \rho + \rho^4 + \rho^9 + \dots + \rho^{(n-1)^2}, \\ \mathfrak{A} &= \frac{1 + A + A^4 + A^9 + \dots + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \dots + \alpha^{(a-1)^2}}, \\ \mathfrak{B} &= \frac{1 + B + B^4 + B^9 + \dots + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \dots + \beta^{(b-1)^2}}, \\ \mathfrak{C} &= \frac{1 + C + C^4 + C^9 + \dots + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \dots + \gamma^{(c-1)^2}}, \\ &\dots \end{aligned}$$

Но первый сомножитель  $w$  определен выше, в исследованиях п. 19, а остальные сомножители получаются из формул пп. 22 и 24, которые мы здесь приведем еще раз, чтобы иметь их все вместе\*. Здесь нужно различать следующие двенадцать случаев.

I. Если  $a$  равно или (нечетному) простому числу  $p$ , или его степени с нечетным показателем, и  $k$  является квадратичным вычетом по модулю  $p$ , то соответствующий сомножитель  $\mathfrak{A}$  равен  $+1$ .

II. Если при тех же остальных предположениях  $k$  является квадратичным невычетом по модулю  $p$ , то  $\mathfrak{A} = -1$ .

III. Если  $a$  является квадратом нечетного простого числа или более высокой его степенью с четным показателем, то  $\mathfrak{A} = +1$ .

IV. Если  $a = 4$  или  $a$  является более высокой степенью числа 2 с четным показателем и одновременно  $k$  имеет вид  $4\mu + 1$ , то  $\mathfrak{A} = +1$ .

V. Если при тех же, что и в IV, остальных предположениях число  $k$  имеет вид  $4\mu + 3$ , а число  $n/a$  — вид  $4\mu + 1$ , то  $\mathfrak{A} = -i$ .

VI. Если при тех же остальных предположениях, что и в IV, число  $k$  имеет вид  $4\mu + 3$ , и число  $n/a$  — также вид  $4\mu + 3$ , то  $\mathfrak{A} = +i$ .

VII. Если  $a = 8$  или  $a$  является более высокой степенью числа 2 с нечетным показателем, и  $k$  имеет вид  $8\mu + 1$ , то  $\mathfrak{A} = +1$ .

VIII. Если при тех же, что и в VII, остальных предположениях  $k$  имеет вид  $8\mu + 5$ , то  $\mathfrak{A} = -1$ .

---

\* Очевидно, что то, что ранее обозначалось через  $k$ ,  $h$ , теперь есть  $n/a$  и  $k$  для второго сомножителя,  $n/b$  и  $k$  для третьего сомножителя и т. д.

IX. Если при тех же, что и в VII, остальных предположениях число  $k$  имеет вид  $8\mu + 3$ , а число  $n/a$  — вид  $4\mu + 1$ , то  $\mathfrak{A} = +i$ .

X. Если при тех же, что и в VII, остальных предположениях число  $k$  имеет вид  $8\mu + 3$ , а число  $n/a$  — вид  $4\mu + 3$ , то  $\mathfrak{A} = -i$ .

XI. Если при тех же, что и в VII, остальных предположениях число  $k$  имеет вид  $8\mu + 7$ , а число  $n/a$  — вид  $4\mu + 1$ , то  $\mathfrak{A} = -i$ .

XII. Если при тех же, что и в VII, остальных предположениях число  $k$  имеет вид  $8\mu + 7$ , а число  $n/a$  — вид  $4\mu + 3$ , то  $\mathfrak{A} = +i$ .

Случай, когда  $a = 2$ , мы пропустили; хотя здесь для  $\mathfrak{A}$  получилось бы выражение  $0/0$ , т. е. неопределенность, однако, всегда  $W = 0$ .

Остальные сомножители  $\mathfrak{B}, \mathfrak{C}, \dots$  так же зависят от  $b, c, \dots$  (если последние фигурируют в определении первых), как  $\mathfrak{A}$  зависит от  $a$ .

### 31

При помощи этого второго метода первый пример из п. 29 решается следующим образом.

Сомножитель  $w$  будет равен  $(1 + i)\sqrt{2520}$ .

Для  $a = 8$ , согласно случаю VIII, соответствующий сомножитель  $\mathfrak{A}$  равен  $-1$ .

Сомножителю 9 числа  $n$  соответствует, согласно случаю III, сомножитель  $+1$ .

Сомножителю 5 соответствует сомножитель  $-1$  (согласно случаю II).

Сомножителю 7 соответствует сомножитель  $-1$  (согласно случаю II).

Отсюда для произведения получаем  $W = (-1 - i)\sqrt{2520}$ , как и в п. 29.

### 32

Так как значение  $W$  может быть определено при помощи двух методов, один из которых основывается на квадратичных характерах чисел  $nk/a, nk/b, nk/c, \dots$  соответственно по модулям  $a, b, c, \dots$

а другой зависит от квадратичных характеров числа  $k$  по модулям  $a, b, c, \dots$ , то между всеми этими квадратичными характеристиками должна существовать некоторая взаимообуславливающая связь, в том смысле, что каждый из этих характеров должен определяться через остальные. Пусть  $a, b, c, \dots$  — нечетные простые числа и  $k = 1$ , далее, сомножители  $a, b, c, \dots$  мы разобьем на два класса, один из которых содержит те сомножители, которые имеют вид  $4\mu + 1$  и которые мы будем обозначать через  $p, p', p'', \dots$ , а второй состоит из тех сомножителей, которые имеют вид  $4\mu + 3$ , и которые мы будем обозначать через  $q, q', q'', \dots$ . Количество последних мы обозначим через  $m$ . После этого заметим, что  $n$  будет иметь вид  $4\mu + 1$ , если  $m$  четно (сюда же следует отнести и случай, когда сомножителей второго класса вообще нет, и потому  $m = 0$ ), и что, напротив,  $n$  будет иметь вид  $4\mu + 3$ , если  $m$  нечетно. Теперь при помощи первого метода  $W$  определяется следующим образом.

Пусть числа  $P, P', P'', \dots, Q, Q', Q'', \dots$  так определяются соответственно отношениями чисел  $n/p, n/p', n/p'', \dots, n/q, n/q', n/q'', \dots$  к числам  $p, p', p'', \dots, q, q', q'', \dots$ , что  $P = +1$ , если  $n/p$  является квадратичным вычетом по модулю  $p$ ,  $P = -1$ , если  $n/p$  является квадратичным невычетом по модулю  $p$ , и точно так же для остальных чисел. Тогда  $W$  является произведением сомножителей  $P\sqrt{p}, P'\sqrt{p'}, P''\sqrt{p''}, \dots, iQ\sqrt{q}, iQ'\sqrt{q'}, iQ''\sqrt{q''}, \dots$ , и потому

$$W = PP'P'' \dots QQ'Q'' \dots i^m \sqrt{n}.$$

При помощи второго метода или даже непосредственно на основании правил п. 19 получается, что

$$W = +\sqrt{n}, \text{ если } n \text{ имеет вид } 4\mu + 1, \text{ или, что то же самое,} \\ \text{если } m \text{ четно,}$$

$$W = +i\sqrt{n}, \text{ если } n \text{ имеет вид } 4\mu + 3, \text{ или, что то же самое,} \\ \text{если } m \text{ нечетно.}$$

Оба эти случая можно одновременно охватить следующей формулой:

$$W = i^{m^2} \sqrt{n}.$$

Итак, из сказанного следует, что

$$PP'P'' \dots QQ'Q'' \dots = i^{m^2-m}.$$

Но  $i^{m^2-m} = 1$ , если  $m$  имеет вид  $4\mu$  или  $4\mu + 1$ , и  $i^{m^2-m} = -1$ , если  $m$  имеет вид  $4\mu + 2$  или  $4\mu + 3$ ; таким образом, мы получаем очень изящную теорему.

**Теорема.** Если  $a, b, c, \dots$  обозначают различные положительные нечетные простые числа, произведение которых равно  $n$  и среди которых имеется  $t$  чисел вида  $4\mu + 3$ , а остальные имеют вид  $4\mu + 1$ , то количество тех из всех этих чисел  $a, b, c, \dots$ , по которым являются невычетами соответственно числа  $n/a, n/b, n/c, \dots$ , четно, если  $t$  имеет вид  $4\mu$  или  $4\mu + 1$ , и нечетно, если  $t$  имеет вид  $4\mu + 2$  или  $4\mu + 3$ .

Так, например, если положить  $a = 3, b = 5, c = 7, d = 11$ , то имеется три числа вида  $4\mu + 3$ , именно, числа 3, 7 и 11. Но  $5 \cdot 7 \cdot 11 R 3; 3 \cdot 7 \cdot 11 R 5; 3 \cdot 5 \cdot 11 R 7; 3 \cdot 5 \cdot 7 N 11$ , т. е. только  $n/d$  является невычетом по модулю  $d$ .

### 33

Знаменитая фундаментальная теорема о квадратичных вычетах представляет собой ни что иное, как специальный случай только что изложенной теоремы. Именно, если мы ограничим количество чисел  $a, b, c, \dots$  двумя, то если вид  $4\mu + 3$  имеет или только одно из них, или ни одного, очевидно будет иметь место либо одновременно  $aRb, bRa$ , либо одновременно  $aNb, bNa$ ; если же оба числа имеют вид  $4\mu + 3$ , то одно из них будет невычетом по другому, а второе будет вычетом по первому. Таким образом, мы имеем здесь четвертое доказательство этой в высшей степени важной теоремы; первое и второе доказательства мы опубликовали в «Арифметических исследованиях», третье, недавно, в отдельном сочинении («Новое доказательство одной арифметической теоремы»); еще два доказательства, которые опять-таки основываются на совершенно иных принципах, мы изложим позднее. Весьма удивительно, что эта прекрасная теорема, которая сначала так упорно сопротивлялась всем попыткам ее доказать, позднее оказалась доступной столь многим совершенно различным подходам.

Также и остальные теоремы, образующие как бы дополнение к фундаментальной теореме, а именно, те, на основании которых можно узнавать, по каким простым числам являются вычетами или невычетами числа  $-1$ ,  $+2$  и  $-2$ , могут быть выведены из этих же принципов. Мы начнем с вычета  $+2$ .

Если положить  $n = 8a$ , где  $a$  является простым числом, и  $k = 1$ , то на основании п. 28  $W$  будет произведением двух сомножителей, один из которых равен  $+\sqrt{a}$  или  $+i\sqrt{a}$  в случае, если число 8 или, что то же самое, число 2 является квадратичным вычетом по модулю  $a$ , и, напротив, равен  $-\sqrt{a}$  или  $-i\sqrt{a}$  в случае, если число 2 является невычетом по модулю  $a$ . Второй же сомножитель равен

$$\begin{aligned} & (1+i)\sqrt{8}, \text{ если } a \text{ имеет вид } 8\mu+1; \\ & (-1+i)\sqrt{8}, \text{ если } a \text{ имеет вид } 8\mu+3; \\ & (-1-i)\sqrt{8}, \text{ если } a \text{ имеет вид } 8\mu+5; \\ & (1-i)\sqrt{8}, \text{ если } a \text{ имеет вид } 8\mu+7. \end{aligned}$$

Но согласно п. 18. всегда  $W = (1+i)\sqrt{n}$ ; если разделить это значение на четыре значения второго сомножителя, то мы получим, что первый сомножитель должен быть равен

$$\begin{aligned} & +\sqrt{a}, \text{ если } a \text{ имеет вид } 8\mu+1; \\ & -i\sqrt{a}, \text{ если } a \text{ имеет вид } 8\mu+3; \\ & -\sqrt{a}, \text{ если } a \text{ имеет вид } 8\mu+5; \\ & +i\sqrt{a}, \text{ если } a \text{ имеет вид } 8\mu+7. \end{aligned}$$

Отсюда непосредственно следует, что в первом и четвертом случаях число 2 должно быть квадратичным вычетом по модулю  $a$ , а во втором и третьем случаях — квадратичным невычетом.

Простые числа, по которым является вычетом или невычетом число  $-1$ , легко можно узнавать при помощи следующей теоремы, которая и сама по себе достойна внимания.



**Теорема.** *Произведение двух сомножителей*

$$W' = 1 + r^{-1} + r^{-4} + \dots + r^{-(n-1)^2},$$
$$W = 1 + r + r^4 + \dots + r^{(n-1)^2}$$

или равно  $n$ , если  $n$  нечетно, или равно  $0$ , если  $n$  четно, но не делится на  $4$ , или равно  $2n$ , если  $n$  делится на  $4$ .

**Доказательство.** Так как, очевидно, имеет место

$$W = r + r^4 + r^9 + \dots + r^{n^2} =$$
$$= r^4 + r^9 + \dots + r^{(n+1)^2} =$$
$$= r^9 + r^{16} + \dots + r^{(n+2)^2}$$

и т. д.,

то произведение  $WW'$  может быть представлено также следующим образом:

$$1 + r + r^4 + r^9 + \dots + r^{(n-1)^2} +$$
$$+ r^{-1}(r + r^4 + r^9 + r^{16} + \dots + r^{n^2}) +$$
$$+ r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \dots + r^{(n+1)^2}) +$$
$$+ r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \dots + r^{(n+2)^2}) +$$
$$\dots$$
$$+ r^{-(n-1)^2}(r^{(n-1)^2} + r^{n^2} + r^{(n+1)^2} + r^{(n+2)^2} + \dots + r^{(2n-2)^2}),$$

и если суммировать по вертикальным рядам, это выражение дает

$$n +$$
$$+ r(1 + r^2 + r^4 + r^6 + \dots + r^{2n-2}) +$$
$$+ r^4(1 + r^4 + r^8 + r^{12} + \dots + r^{4n-4}) +$$
$$+ r^9(1 + r^6 + r^{12} + r^{18} + \dots + r^{6n-6}) +$$
$$\dots$$
$$+ r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \dots + r^{2(n-1)^2}).$$

Если теперь  $n$  нечетно, то отдельные части этой суммы, кроме первой, равной  $n$ , равны  $0$ ; действительно, вторая часть будет,

очевидно, равна  $\frac{r(1-r^{2n})}{1-r^2}$ , третья равна  $\frac{r^4(1-r^{4n})}{1-r^4}$  и т. д. Если же  $n$  четно, то нужно исключить еще и часть

$$r^{n^2/4}(1 + r^n + r^{2n} + r^{3n} + \dots + r^{n^2-n}).$$

которая равна  $nr^{n^2/4}$ .

Таким образом, в первом случае  $WW' = n$ , а во втором случае  $WW' = n + nr^{n^2/4}$ ; но  $r^{n^2/4} = +1$ , если  $n$  делится на 4, и тогда следовательно,  $WW' = 2n$ ; напротив, если  $n$  четно, но не делится на 4, то  $r^{n^2/4} = -1$  и потому в этом случае  $WW' = 0$ .

### 36

Из п. 22 мы знаем, что если  $n$  является нечетным простым числом, то либо  $\frac{W'}{W} = +1$ , либо  $\frac{W'}{W} = -1$ , в зависимости от того, является ли число  $-1$  вычетом или невычетом по модулю  $n$ . Поэтому в первом случае должно быть  $W^2 = +n$ , а во втором  $W^2 = -n$ . Поэтому на основании п. 13 мы заключаем, что первый случай может иметь место только тогда, когда  $n$  имеет вид  $4\mu + 1$ , а второй — только тогда, когда  $n$  имеет вид  $4\mu + 3$ .

Наконец, комбинируя условия, найденные для вычетов  $+2$  и  $-1$ , мы сразу получаем, что число  $-2$  является вычетом по каждому простому числу вида  $8\mu + 1$  или  $8\mu + 3$  и невычетом по каждому простому числу вида  $8\mu + 5$  или  $8\mu + 7$ .

---

# НОВЫЕ ДОКАЗАТЕЛЬСТВА И ОБОБЩЕНИЯ ФУНДАМЕНТАЛЬНОЙ ТЕОРЕМЫ В УЧЕНИИ О КВАДРАТИЧНЫХ ВЫЧЕТАХ

*(Commentationes soc. red. sc. Gotting.  
recentiores, Vol. IV, Gotting, 1818)*

Хотя фундаментальную теорему о квадратичных вычетах, которая принадлежит к прекраснейшим истинам высшей арифметики, легко было обнаружить индуктивным путем, доказать ее оказалось значительно труднее. При исследованиях такого рода чаще оказывается, что доказательства простейших фактов, которые в большинстве случаев кажутся исследователю очевидными с первого взгляда, оказываются скрытыми очень глубоко и извлекаются на свет лишь после многих тщетных попыток, причем совсем не таким путем, на котором их раньше искали. Далее, не редко случается, что после того как был найден *один* путь, тотчас же открывается и *несколько* путей, ведущих к той же цели, одни из которых короче и прямее, другие же приводят к цели как будто со стороны и основываются на совершенно отличных принципах, между которыми и предметом исследования почти нельзя было предположить никакой связи. Такая замечательная связь между скрытыми закономерностями не только придает этим исследованиям некоторую своеобразную привлекательность, но и заслуживает тщательного выяснения, так как нередко благодаря ей открываются новые возможности для развития науки.

Таким образом, хотя рассматриваемая здесь арифметическая теорема могла бы показаться совершенно исчерпанной благодаря пре-

дыдущим усилиям, которые уже доставили четыре \* во всех отношениях отличных одно от другого ее доказательства, я тем не менее снова возвращаюсь к этому же предмету и предлагаю еще два доказательства, которые проливают на этот вопрос новый свет. Первое из них, правда, родственно третьему доказательству в том отношении, что исходит из той же леммы; в дальнейшем, однако, оно идет другим путем, так что его по праву можно считать новым доказательством, которое если не короче третьего, то и не длиннее. Шестое же доказательство основывается на совершенно отличном от остальных очень тонком принципе и дает новый пример замечательной связи между арифметическими фактами, которые на первый взгляд лежат очень далеко один от другого. К этим двум доказательствам мы добавляем еще новый очень простой алгоритм, для того чтобы узнавать, является ли заданное целое число квадратичным вычетом или невычетом по заданному простому числу.

Была еще и другая причина, которая заставила меня только теперь опубликовать новые доказательства, о которых я говорил еще девять лет назад. Именно, когда я в 1805 г. начал исследовать теорию кубических и биквадратичных вычетов,— предмет намного более трудный,— меня постигла почти такая же судьба, как когда-то в теории квадратичных вычетов. Именно, теоремы, которые полностью исчерпывали рассматриваемые вопросы, и в которых проявляется замечательная аналогия с теоремами, касающимися квадратичных вычетов, сразу находились индуктивно, как только их искали на правильном пути, но все попытки достигнуть во всех отношениях совершенных доказательств, долгое время оставались тщетными. Это как раз и явилось стимулом к тому, что я к уже известным доказательствам относительно квадратичных вычетов старался добавить все новые и новые, в надежде, что какой-нибудь из многих различных методов может прибавить что-либо к выяснению родственного вопроса. Эта надежда оказалась отнюдь не напрасной, и неутомимая работа увенчалась наконец успехом. Вскоре я буду в

---

\* Два доказательства изложены в четвертом и пятом разделах *«Арифметических исследований»*, третье — в отдельном сочинении *«Новое доказательство одной арифметической теоремы»*, четвертое содержится в сочинении *«Суммирование некоторых рядов особого вида»*.

состоянии опубликовать результаты моих исследований; однако, прежде чем приступить к этому трудному делу, я решил еще раз вернуться к теории квадратичных вычетов, изложить все, что относительно нее еще осталось сказать, и в известном смысле распространиться с этой частью высшей арифметики.

## Пятое доказательство фундаментальной теоремы теории квадратичных вычетов

### 1

Во введении мы уже говорили, что пятое и третье доказательства исходят из одной и той же леммы, которую мы здесь для удобства повторим в обозначениях, целесообразных для настоящего исследования.

**Лемма.** Пусть  $m$  — положительное нечетное простое число,  $M$  — целое число, не делящееся на  $m$ ; возьмем наименьшие положительные вычеты по модулю  $m$  чисел

$$M, 2M, 3M, 4M, \dots, \frac{1}{2}(m-1)M;$$

часть этих вычетов будет меньше, а часть больше чем  $m/2$ ; пусть количество последних равно  $n$ . Тогда  $M$  будет квадратичным вычетом или невычетом по модулю  $m$  в зависимости от того, четно число  $n$  или нечетно.

**Доказательство.** Если  $a, b, c, d, \dots$  — те из наших вычетов, которые меньше чем  $m/2$ , и  $a', b', c', d', \dots$  — остальные вычеты, которые больше чем  $m/2$ , то дополнения последних до  $m$ , т. е. числа  $m - a', m - b', m - c', m - d', \dots$  будут, очевидно, все меньше чем  $m/2$  и будут отличны как одно от другого, так и от вычетов  $a, b, c, d, \dots$ , так что вместе с этими вычетами они, быть может только в другом порядке, будут образовывать совокупность всех чисел  $1, 2, 3, 4, \dots, \dots, (m-1)/2$ . Поэтому, если положить

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot \frac{1}{2}(m-1) = P,$$

то будет выполняться равенство

$$P = abcd \dots (m - a') (m - b') (m - c') (m - d') \dots,$$

и потому

$$(-1)^n P = abcd \dots (a' - m) (b' - m) (c' - m) (d' - m) \dots$$

Далее, по модулю  $m$  будет иметь место

$$PM^{(m-1)/2} \equiv abcd \dots a'b'c'd' \dots \equiv abcd \dots (a' - m) (b' - m) (c' - m) (d' - m) \dots,$$

и потому

$$PM^{(m-1)/2} \equiv P (-1)^n.$$

Следовательно,  $M^{(m-1)/2} \equiv \pm 1$ , где нужно брать верхний или нижний знак в зависимости от того, четно  $n$  или нечетно, а отсюда справедливость нашей леммы сразу вытекает на основании теоремы, доказанной в «Арифметических исследованиях», п. 106.

## 2

**Теорема.** Пусть  $m, M$  — положительные нечетные взаимно простые числа,  $n$  — количество тех вычетов среди наименьших положительных вычетов по модулю  $m$  чисел

$$M, 2M, 3M, \dots, \frac{1}{2} (m - 1) M,$$

которые больше чем  $m/2$ , и точно так же  $N$  — количество тех вычетов среди наименьших положительных вычетов по модулю  $M$  чисел

$$m, 2m, 3m, \dots, \frac{1}{2} (M - 1) m,$$

которые больше чем  $M/2$ ; тогда три числа  $n, N, (m-1)(M-1)/4$  или все четны, или одно из них четно, а два другие нечетны.

**Доказательство.** Обозначим

через  $f$  совокупность чисел  $1, 2, 3, \dots, (m-1)/2$ ,

через  $f'$  совокупность чисел  $m-1, m-2, m-3, \dots, (m+1)/2$ ,

через  $F$  совокупность чисел  $1, 2, 3, \dots, (M-1)/2$ ,

через  $F'$  совокупность чисел  $M-1, M-2, M-3, \dots, (M+1)/2$ .

Таким образом, число  $n$  будет показывать, сколько чисел среди  $Mf$  имеют свои наименьшие положительные вычеты по модулю  $m$  в совокупности  $f'$ , и точно так же число  $N$  будет показывать, сколько чисел среди  $mF$  имеют свои наименьшие положительные вычеты по модулю  $M$  в совокупности  $F'$ . Наконец, обозначим через  $\varphi$  совокупность чисел  $1, 2, 3, \dots, (mM - 1)/2$ , через  $\varphi'$  совокупность чисел  $mM - 1, mM - 2, mM - 3, \dots, (mM + 1)/2$ .

Так как каждое целое не делящееся на  $m$  число должно быть сравнимо по модулю  $m$  либо с каким-нибудь вычетом из  $f$ , либо с каким-нибудь вычетом из  $f'$ , и точно так же каждое целое не делящееся на  $M$  число сравнимо по модулю  $M$  либо с каким-нибудь вычетом из  $F$ , либо с каким-нибудь вычетом из  $F'$ , то все числа совокупности  $\varphi$ , среди которых, очевидно, нет чисел, делящихся одновременно на  $m$  и  $M$ , можно следующим образом разбить на восемь классов.

I. В первом классе находятся числа, которые по модулю  $m$  сравнимы с каким-нибудь числом из  $f$ , а по модулю  $M$  — с каким-нибудь числом из  $F$ . Количество этих чисел мы обозначим через  $\alpha$ .

II. Вторым классом содержат числа, которые по модулям  $m, M$  сравнимы соответственно с числами из  $f, F'$ . Количество этих чисел мы положим равным  $\beta$ .

III. Третьим классом содержат числа, которые по модулям  $m, M$  сравнимы соответственно с числами из  $f', F$ . Их количество мы положим равным  $\gamma$ .

IV. Четвертым классом содержат числа, которые по модулям  $m, M$  сравнимы соответственно с числами из  $f', F'$ . Их количество пусть равно  $\delta$ .

V. Пятым классом содержат числа, которые делятся на  $m$ , а по модулю  $M$  сравнимы с вычетами из  $F$ .

VI. Шестым классом содержат числа, которые делятся на  $m$ , а по модулю  $M$  сравнимы с вычетами из  $F'$ .

VII. Седьмым классом содержат числа, которые делятся на  $M$ , а по модулю  $m$  сравнимы с вычетами из  $f$ .

VIII. Восьмым классом содержат числа, которые делятся на  $M$ , а по модулю  $m$  сравнимы с вычетами из  $f'$ .

Очевидно, что классы V и VI вместе охватывают всевозможные

числа  $mF$ ; но количество чисел, содержащихся в VI, равно  $N$ , поэтому количество чисел, содержащихся в V, равно  $\frac{1}{2}(M-1)-N$ . Точно так же классы VII и VIII вместе содержат всевозможные числа  $Mf$ ; в классе VIII находится  $n$  чисел, а в классе VII находится  $\frac{1}{2}(m-1)-n$  чисел.

Совершенно аналогичным образом все числа совокупности  $\varphi'$  распадаются на восемь классов IX — XVI; если при разбиении этих чисел мы будем придерживаться прежнего порядка, то числа, содержащиеся в классах

IX, X, XI, XII, XIII, XIV, XV, XVI,

будут, очевидно, дополнениями до  $mM$  чисел, содержащихся соответственно в классах

IV, III, II, I, VI, V, VIII, VII,

так что в классе IX будет находиться  $\delta$  чисел, в классе X будет находиться  $\gamma$  чисел и т. д. Но ясно, что если объединить все числа первого класса со всеми числами девятого класса, то получатся все числа, меньшие чем  $mM$ , которые по модулю  $m$  сравнимы с некоторым числом из  $f$ , а по модулю  $M$  — с некоторым числом из  $F$ , и легко видеть, что количество их равно количеству всех комбинаций отдельных чисел из  $f$  с отдельными числами из  $F$ . Поэтому мы имеем, что

$$\alpha + \delta = \frac{1}{4}(m-1)(M-1),$$

и по аналогичной причине

$$\beta + \gamma = \frac{1}{4}(m-1)(M-1).$$

Если собрать вместе все числа из классов II, IV, VI, то мы получим, очевидно, все числа, меньшие чем  $mM/2$ , которые сравнимы по модулю  $M$  с некоторым вычетом из  $F'$ . Но эти же числа могут быть представлены и в виде

$$F', M + F', 2M + F', 3M + F', \dots, \frac{1}{2}(m-3)M + F',$$



так что количество их равно  $(m-1)(M-1)/4$ , т. е. мы имеем, что

$$\beta + \delta + N = \frac{1}{4}(m-1)(M-1).$$

Точно так же, собирая вместе все числа классов III, IV, VIII, можно заключить, что

$$\gamma + \delta + n = \frac{1}{4}(m-1)(M-1).$$

Из этих четырех уравнений мы получаем следующие:

$$2\alpha = \frac{1}{4}(m-1)(M-1) + n + N,$$

$$2\beta = \frac{1}{4}(m-1)(M-1) + n - N,$$

$$2\gamma = \frac{1}{4}(m-1)(M-1) - n + N,$$

$$2\delta = \frac{1}{4}(m-1)(M-1) - n - N,$$

каждое из которых доказывает справедливость теоремы.

### 3

Если мы теперь предположим, что  $m$  и  $M$  — простые числа, то из соединения настоящей теоремы с леммой из п. 1 тотчас же получается *фундаментальная теорема*. Действительно, ясно,

I) что если каждое из чисел  $m$ ,  $M$  или только одно из них имеет вид  $4k+1$ , то число  $\frac{1}{4}(m-1)(M-1)$  четно, и потому числа  $n$ ,  $N$  или одновременно четны, или одновременно нечетны, т. е. либо каждое из чисел  $m$  и  $M$  является квадратичным вычетом по другому из них, либо каждое является квадратичным невычетом по другому;

II) если же оба числа  $m$ ,  $M$  имеют вид  $4k+3$ , то  $(m-1)(M-1)/4$  является нечетным числом, а потому одно из чисел  $n$ ,  $N$  четно, а другое нечетно, и тем самым одно из чисел  $m$ ,  $M$  есть квадратичный вычет по другому, а второе есть квадратичный невычет по первому.

## Шестое доказательство фундаментальной теоремы теории квадратичных вычетов

### 1

**Теорема.** Если  $p$  обозначает (положительное нечетное) простое число,  $n$  — целое положительное число, не делящееся на  $p$ , и  $x$  — переменную величину, то функция

$$1 + x^n + x^{2n} + x^{3n} + \dots + x^{np-n}$$

делится на функцию

$$1 + x + x^2 + x^3 + \dots + x^{p-1}.$$

**Доказательство.** Если взять такое целое положительное число  $g$ , что  $gn \equiv 1 \pmod{p}$ , и положить  $gn = 1 + hp$ , то

$$\begin{aligned} \frac{1 + x^n + x^{2n} + x^{3n} + \dots + x^{np-n}}{1 + x + x^2 + x^3 + \dots + x^{p-1}} &= \frac{(1 - x^{np})(1 - x)}{(1 - x^n)(1 - x^p)} = \\ &= \frac{(1 - x^{np})(1 - x^{gn} - x + x^{hp+1})}{(1 - x^n)(1 - x^p)} = \\ &= \frac{1 - x^{np}}{1 - x^p} \cdot \frac{1 - x^{gn}}{1 - x^n} - \frac{x(1 - x^{np})}{1 - x^n} \cdot \frac{1 - x^{hp}}{1 - x^p}, \end{aligned}$$

и потому стоящая слева функция, очевидно, будет целой, что и требовалось доказать.

Таким образом, каждая целая функция от  $x$ , которая делится на  $(1 - x^{np}) / (1 - x^n)$ , делится также и на  $(1 - x^p) / (1 - x)$ .

### 2

Обозначим через  $\alpha$  положительный первообразный корень по модулю  $p$ , т. е. положительное целое число с тем свойством, что наименьшие положительные вычеты по модулю  $p$  степеней  $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{p-2}$  с точностью до порядка расположения совпадают с числами  $1, 2, 3, 4, \dots, p-1$ . Если обозначить далее через  $f(x)$  функцию

$$x + x^\alpha + x^{\alpha^2} + x^{\alpha^3} + \dots + x^{\alpha^{p-2}} + 1,$$

3

[illegible]

Тем самым это выражение  $\Omega$  делится также и на  $(1 - x^p)/(1 - x)$ . Но среди показателей  $2, \alpha + 1, \alpha^2 + 1, \alpha^3 + 1, \dots, \alpha^{p-2} + 1$  только

один, а именно,  $\alpha^{(p-1)/2} + 1$ , делится на  $p$ , так что, согласно предыдущему пункту, на  $(1 - x^p)/(1 - x)$  делятся все отдельные части  $f(x^2), f(x^{\alpha+1}), f(x^{\alpha^2+1}), f(x^{\alpha^3+1}), \dots$  выражения  $\Omega$ , за исключением лишь члена  $f(x^{\alpha^{(p-1)/2}+1})$ . Поэтому указанные части можно отбросить, так что делящейся на  $(1 - x^p)/(1 - x)$  остается функция

$$\xi^2 \mp f(x^{\alpha^{(p-1)/2}+1}),$$

где берется верхний или нижний знак в зависимости от того, имеет ли  $p$  вид  $4k + 1$  или  $4k + 3$ . А так как, кроме того,  $f(x^{\alpha^{(p-1)/2}+1}) - p$  делится на  $(1 - x^p)/(1 - x)$ , то и  $\xi^2 \mp p$  будет делиться на  $(1 - x^p)/(1 - x)$ . Это и требовалось доказать.

Для того, чтобы двойной знак не приводил ни к какой неопределенности, мы обозначим через  $\varepsilon$  число, равное  $+1$  или  $-1$  в зависимости от того, имеет ли  $p$  вид  $4k + 1$  или вид  $4k + 3$ . Тогда  $(1 - x)(\xi^2 - \varepsilon p)/(1 - x^p)$  будет целой функцией от  $x$ , которую мы обозначим через  $Z$ .

#### 4

Пусть  $q$  — положительное нечетное число и потому  $(q - 1)/2$  — целое число. Тогда  $(\xi^2)^{(q-1)/2} - (\varepsilon p)^{(q-1)/2}$  будет делиться на  $\xi^2 - \varepsilon p$  и тем самым также и на  $(1 - x^p)/(1 - x)$ . Если мы положим

$$\varepsilon^{(q-1)/2} = \delta \text{ и } \xi^{q-1} - \delta p^{(q-1)/2} = \frac{1 - x^p}{1 - x} Y,$$

то  $Y$  будет целой функцией от  $x$ , а  $\delta = +1$ , если одно из чисел  $p, q$  или оба они имеют вид  $4k + 1$ , и, напротив,  $\delta = -1$ , если оба числа  $p, q$  имеют вид  $4k + 3$ .

#### 5

Если мы предположим теперь, что  $q$  также является простым числом (отличным от  $p$ ), то, согласно доказанной в «Арифметических исследованиях», п. 51, теореме, функция

$$\xi^q - (x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \dots - x^{q\alpha^{p-2}})$$

будет, очевидно, делиться на  $q$ , т. е. будет иметь вид  $qX$ , где  $X$  является функцией от  $x$  с целыми коэффициентами (что справедливо также и относительно остальных фигурирующих здесь функций  $Z, Y, W$ ). Если для модуля  $p$  и первообразного корня  $\alpha$  мы обозначим через  $\mu$  индекс числа  $q$ , т. е. если  $q \equiv \alpha^\mu \pmod{p}$ , то числа  $q, q\alpha, q\alpha^2, q\alpha^3, \dots, q\alpha^{p-2}$  будут сравнимы по модулю  $p$  соответственно с числами  $\alpha^\mu, \alpha^{\mu+1}, \alpha^{\mu+2}, \dots, \alpha^{p-2}, 1, \alpha, \alpha^2, \dots, \alpha^{\mu-1}$ , и потому

$$\begin{aligned} x^q &= x^{\alpha^\mu}, \\ x^{q\alpha} &= x^{\alpha^{\mu+1}}, \\ x^{q\alpha^2} &= x^{\alpha^{\mu+2}}, \\ x^{q\alpha^3} &= x^{\alpha^{\mu+3}}, \\ &\dots\dots\dots \\ x^{q\alpha^{p-\mu-2}} &= x^{\alpha^{p-2}}, \\ x^{q\alpha^{p-\mu-1}} &= x, \\ x^{q\alpha^{p-\mu}} &= x^\alpha, \\ x^{q\alpha^{p-\mu+1}} &= x^{\alpha^2}, \\ &\dots\dots\dots \\ x^{q\alpha^{p-2}} &= x^{\alpha^{\mu-1}} \end{aligned}$$

делятся на  $1 - x^p$ . Если сложить эти функции, взятые попеременно то положительными, то отрицательными, то станет ясным, что функция

$$x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \dots - x^{q\alpha^{p-2}} \mp \xi$$

делится на  $1 - x^p$ , причем нужно брать верхний или нижний знак в зависимости от того, четно  $\mu$  или нечетно, т. е. в зависимости от того, является ли  $q$  квадратичным вычетом или невычетом по модулю  $p$ . Положим поэтому

$$x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \dots - x^{q\alpha^{p-2}} - \gamma\xi = (1 - x^p) W,$$

где мы предполагаем, что  $\gamma = +1$  или  $= -1$  в зависимости от того, является ли  $q$  квадратичным вычетом или невычетом по модулю  $p$ ; тогда  $W$  будет целой функцией.

После этих приготовлений мы, комбинируя предыдущие уравнения, выводим уравнение

$$q\xi X = \varepsilon p (\delta p^{(q-1)/2} - \gamma) + \frac{1-x^p}{1-x} (Z (\delta p^{(q-1)/2} - \gamma) + Y\xi^2 - W\xi (1-x)).$$

Предположим, что при делении функции  $\xi X$  на

$$x^{p-1} + x^{p-2} + x^{p-3} + \dots + x + 1$$

получаются частное  $U$  и остаток  $T$ , т. е. что

$$\xi X = \frac{1-x^p}{1-x} U + T,$$

так что функции  $U$ ,  $T$  имеют целые коэффициенты, причем  $T$  заведомо имеет степень, меньшую чем делитель. Тогда

$$\begin{aligned} qT - \varepsilon p (\delta p^{(q-1)/2} - \gamma) &= \\ &= \frac{1-x^p}{1-x} [Z (\delta p^{(q-1)/2} - \gamma) + Y\xi^2 - W\xi (1-x) - qU], \end{aligned}$$

а это равенство, очевидно, может выполняться лишь в том случае, когда одновременно обращаются в нуль как левая, так и правая части. Таким образом, на  $q$  делится как  $\varepsilon p (\delta p^{(q-1)/2} - \gamma)$ , так и  $\delta p^{(q-1)/2} - \gamma$ , а так как  $\delta^2 = 1$ , то и число  $p^{(q-1)/2} - \gamma\delta$  делится на  $q$ .

Если мы теперь обозначим через  $\beta$  единицу, взятую с положительным или отрицательным знаком в зависимости от того, является ли  $p$  квадратичным вычетом или невычетом по модулю  $q$ , то на  $q$  будет делиться число  $p^{(q-1)/2} - \beta$ , а потому также и  $\beta - \gamma\delta$ ; но это возможно лишь в том случае, если  $\beta = \gamma\delta$ . Из этого тотчас же следует фундаментальная теорема. Именно,

I) если либо каждое из чисел  $p$ ,  $q$ , либо по крайней мере одно из них имеет вид  $4k+1$ , и потому  $\delta = +1$ , то будет иметь место  $\beta = \gamma$ , и потому либо одновременно  $q$  является квадратичным вычетом по модулю  $p$  и  $p$  — квадратичным вычетом по модулю  $q$ , либо одновременно  $q$  есть квадратичный невычет по модулю  $p$ , и  $p$  — квадратичный невычет по модулю  $q$ ;

II) если оба числа  $p$ ,  $q$  имеют вид  $4k+3$ , и потому  $\delta = -1$ , то будет иметь место  $\beta = -\gamma$ , и потому либо одновременно  $q$

является квадратичным вычетом по модулю  $p$ , и  $p$  — квадратичным невычетом по модулю  $q$ , либо одновременно  $q$  есть невычет по модулю  $p$ , а  $p$  — вычет по модулю  $q$ . Это и требовалось доказать.

**Новый алгоритм для определения того, является ли заданное положительное целое число квадратичным вычетом или невычетом по заданному положительному простому модулю**

# 1

Прежде чем изложить новое решение этой задачи, мы хотим кратко повторить здесь решение, данное в *«Арифметических исследованиях»*, так как оно довольно просто может быть проведено при помощи фундаментальной теоремы и следующих известных теорем.

I. Отношение числа  $a$  к числу  $b$  (в том смысле, является ли первое квадратичным вычетом или невычетом по второму) является таким же, как и отношение числа  $c$  к числу  $b$ , если  $a \equiv c \pmod{b}$ .

II. Если  $a$  является произведением сомножителей  $\alpha, \beta, \gamma, \delta, \dots$ , и  $b$  — простое число, то отношение числа  $a$  к числу  $b$  так зависит от отношений этих сомножителей к числу  $b$ , что  $a$  является квадратичным вычетом или невычетом по модулю  $b$  в зависимости от того, четно или нечетно количество сомножителей, которые являются невычетами по модулю  $b$ . Таким образом, если какой-нибудь из сомножителей является квадратом, то его при исследовании можно вообще не принимать во внимание; если же какой-нибудь из сомножителей является степенью некоторого целого числа с нечетным показателем, то вместо степени можно взять само это целое число.

III. Число 2 является квадратичным вычетом по каждому простому числу вида  $8m + 1$  или  $8m + 7$ , и, напротив, невычетом по каждому простому числу вида  $8m + 3$  или  $8m + 5$ .

Если поэтому дано число  $a$  и отыскивается его отношение к простому числу  $b$ , то прежде всего вместо числа  $a$ , если оно больше чем  $b$ , берется его наименьший положительный вычет по модулю  $b$ , и если этот вычет разложен на простые сомножители, то, согласно теореме II, задача сводится к нахождению отношений к числу  $b$  для этих отдельных сомножителей. Отношение сомножителя 2 (если он входит

один раз, или три раза, или пять раз и т. д.) известно на основании теоремы III; отношение же остальных сомножителей в силу фундаментальной теоремы зависит от отношения  $b$  к отдельным сомножителям. Таким образом, вместо одного отношения заданного числа к простому числу  $b$  получается теперь несколько отношений числа  $b$  к другим нечетным простым числам, которые меньше чем  $b$ , а эти задачи таким же способом сводятся к еще меньшим модулям, причем эти последовательные редукции, очевидно, рано или поздно будут иметь конец.

## 2

Чтобы пояснить это решение примером, найдем отношение числа 103 к числу 379. Так как число 103 уже меньше чем 379 и само является простым числом, то сразу же применяется фундаментальная теорема, которая показывает, что искомое отношение противоположно отношению числа 379 к числу 103. Последнее в свою очередь равно отношению числа 70 к числу 103, которое зависит от отношений к числу 103 чисел 2, 5, 7. Первое из этих отношений известно на основании теоремы III. Второе, согласно фундаментальной теореме, зависит от отношения числа 103 к числу 5, которое, по теореме I, совпадает с отношением числа 3 к числу 5; последнее, на основании фундаментальной теоремы, в свою очередь зависит от отношения числа 5 к числу 3, которое, по теореме I, совпадает с отношением числа 2 к числу 3, известным по теореме III. Точно так же отношение числа 7 к числу 103, на основании фундаментальной теоремы зависит от отношения числа 103 к числу 7, которое, в силу теоремы I, совпадает с отношением числа 5 к числу 7; последнее, согласно фундаментальной теореме, в свою очередь зависит от отношения числа 7 к числу 5, которое, по теореме I, совпадает с отношением числа 2 к числу 5, известному на основании теоремы III. Если теперь представить этот анализ синтетически, то ответ на вопрос будет зависеть от четырнадцати отдельных моментов, которые мы здесь приведем полностью, чтобы сделать еще более очевидной краткость нового решения.

1. Число 2 является квадратичным вычетом по числу 103 (теорема III).



2. Число 2 является квадратичным невычетом по числу 3 (теорема III).
3. Число 5 является квадратичным невычетом по числу 3 (по теореме I и 2).
4. Число 3 является квадратичным невычетом по числу 5 (фундаментальная теорема и 3).
5. Число 103 является квадратичным невычетом по числу 5 (теорема I и 4).
6. Число 5 является квадратичным невычетом по числу 103 (фундаментальная теорема и 5).
7. Число 2 является квадратичным невычетом по числу 5 (теорема III).
8. Число 7 является квадратичным невычетом по числу 5 (теорема I и 7).
9. Число 5 является квадратичным невычетом по числу 7 (фундаментальная теорема и 8).
10. Число 103 является квадратичным невычетом по числу 7 (теорема I и 9).
11. Число 7 является квадратичным вычетом по числу 103 (фундаментальная теорема и 10).
12. Число 70 является квадратичным невычетом по числу 103 (теорема II, 1, 6, 11).
13. Число 379 является квадратичным невычетом по числу 103 (теорема I и 12).
14. Число 103 является квадратичным вычетом по числу 379.

В дальнейшем мы ради краткости будем использовать обозначение, введенное в сочинении «*Новое доказательство одной арифметической теоремы*». Именно, мы будем обозначать через  $[x]$  самое величину  $x$ , если  $x$  является целым числом, и, напротив, ближайшее к  $x$  целое число, меньшее чем  $x$ , если  $x$  является дробной величиной, так что  $x - [x]$  всегда будет не отрицательной величиной, меньшей чем 1.

**Задача.** Пусть  $a, b$  обозначают положительные взаимно простые целые числа, и  $\left[\frac{1}{2}a\right] = a'$ ; нужно найти сумму

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \left[\frac{3b}{a}\right] + \left[\frac{4b}{a}\right] + \dots + \left[\frac{a'b}{a}\right].$$

**Решение.** Мы обозначим для краткости подобную сумму через  $\varphi(a, b)$ , так что будет иметь место также и

$$\varphi(b, a) = \left[\frac{a}{b}\right] + \left[\frac{2a}{b}\right] + \left[\frac{3a}{b}\right] + \dots + \left[\frac{b'a}{b}\right],$$

если положить  $\left[\frac{1}{2}b\right] = b'$ . В третьем доказательстве фундаментальной теоремы было показано, что в случае, когда числа  $a$  и  $b$  нечетны, выполняется равенство

$$\varphi(a, b) + \varphi(b, a) = a'b',$$

и тем же методом легко доказать справедливость этой теоремы и в том случае, когда только одно из чисел  $a, b$  нечетно, о чем уже упоминалось в указанном месте. По аналогии с тем способом, которым отыскивается наибольший общий делитель двух целых чисел, разделим число  $a$  на  $b$ ; пусть частное равно  $\beta$ , и остаток равен  $c$ ; затем разделим  $b$  на  $c$  и т. д., так что получим равенства

$$\begin{aligned} a &= \beta b + c, \\ b &= \gamma c + d, \\ c &= \delta d + e, \\ d &= \varepsilon e + f, \\ &\dots \end{aligned}$$

При этом в ряду все время уменьшающихся чисел  $b, c, d, e, f, \dots$ , мы в конце концов придем к единице, ибо числа  $a$  и  $b$  по предположению взаимно просты, так что последним равенством будет

$$k = \lambda l + 1.$$

Но так как, очевидно, имеет место

$$\begin{aligned} \left[\frac{a}{b}\right] &= \left[\beta + \frac{c}{b}\right] = \beta + \left[\frac{c}{b}\right], \\ \left[\frac{2a}{b}\right] &= \left[2\beta + \frac{2c}{b}\right] = 2\beta + \left[\frac{2c}{b}\right], \\ \left[\frac{3a}{b}\right] &= \left[3\beta + \frac{3c}{b}\right] = 3\beta + \left[\frac{3c}{b}\right] \end{aligned}$$

и т. д.,

$$\varphi(b, a) = \varphi(b, c) + \frac{1}{2} \beta(b'^2 + b'),$$
$$\varphi(a, b) = a'b' - \frac{1}{2} \beta (b'^2 + b') - \varphi(b, c).$$

По аналогичной причине, если положить  $\left[\frac{1}{2}c\right] = c'$ ,  $\left[\frac{1}{2}d\right] = d'$ ,  $\left[\frac{1}{2}e\right] = e', \dots$ , то будут выполняться равенства

$$\varphi(b, c) = b'c' - \frac{1}{2}\gamma(c'^2 + c') - \varphi(c, d),$$

$$\varphi(c, d) = c'd' - \frac{1}{2} \delta(d'^2 + d') - \varphi(d, e),$$

$$\varphi(d, e) = d'e' - \frac{1}{2} \varepsilon(e'^2 + e') - \varphi(e, f),$$

• • • • •

$$\varphi(k, l) = k'l' - \frac{1}{2} \lambda (l'^2 + l') - \varphi(l, 1).$$

Отсюда мы получаем (так как, очевидно,  $\varphi(l, 1) = 0$ ) формулу

$$\begin{aligned} \varphi(a, b) = & a'b' - b'c' + c'd' - d'e' + \dots \pm k'l' - \\ & - \frac{1}{2} \beta (b'^2 + b') + \frac{1}{2} \gamma (c'^2 + c') - \frac{1}{2} \delta (d'^2 + d') + \\ & + \frac{1}{2} \varepsilon (e'^2 + e') - \dots \mp \lambda (l'^2 + l'). \end{aligned}$$

4

Из того, что было изложено в третьем доказательстве, легко вывести, что отношение числа  $b$  к  $a$ , в случае, когда число  $a$  простое, немедленно можно узнать по значению суммы  $\varphi(a, 2b)$ : Именно, в зависимости от того, четна эта сумма или нечетна, число  $b$  будет квадратичным вычетом или невычетом по модулю  $a$ . Но для этой же цели может быть использована и сама сумма  $\varphi(a, b)$ , с тем, однако, ограничением, что случай, когда  $b$  нечетно, следует отличать от случая, когда  $b$  четно. Именно,

Г) если  $b$  нечетно, то  $b$  является квадратичным вычетом или невычетом по модулю  $a$  в зависимости от того, четно или нечетно  $\varphi(a, b)$ ;

II) если  $b$  четно, то сохраняет силу это же правило, когда, кроме того,  $a$  имеет вид  $8n + 1$  или  $8n + 7$ ; если же при четном значении числа  $b$  модуль  $a$  имеет вид  $8n + 3$  или  $8n + 5$ , то правило будет противоположным, т. е.  $b$  будет квадратичным вычетом по модулю  $a$ , когда  $\varphi(a, b)$  нечетно, и, напротив, невычетом, когда  $\varphi(a, b)$  четно.

Все это легко получается из п. 4 третьего доказательства.

### 5

**Пример.** Если отыскивается отношение числа 103 к простому числу 379, то для получения суммы  $\varphi(379, 103)$  мы имеем

$$\begin{array}{c|c|c} a = 379 & a' = 189 & \\ b = 103 & b' = 51 & \beta = 3 \\ c = 70 & c' = 35 & \gamma = 1 \\ d = 33 & d' = 16 & \delta = 2 \\ e = 4 & e' = 2 & \varepsilon = 8, \end{array}$$

поэтому

$$\begin{aligned} \varphi(379, 103) &= \\ &= 9639 - 1785 + 560 - 32 - 3978 + 630 - 272 + 24 = 4786, \end{aligned}$$

так что 103 является квадратичным вычетом по числу 379. Если же мы захотим использовать для этой цели сумму  $\varphi(379, 206)$ , то мы будем иметь

$$\begin{array}{c|c|c} 379 & 189 & \\ 206 & 103 & 1 \\ 173 & 86 & 1 \\ 33 & 16 & 5 \\ 8 & 4 & 4, \end{array}$$

откуда получается, что

$$\begin{aligned} \varphi(379, 206) &= 19\,467 - 8858 + 1376 - 64 - 5356 + \\ &\quad + 3741 - 680 + 40 = 9666; \end{aligned}$$

тем самым 103 является квадратичным вычетом по модулю 379.

## 6

Так как для определения отношения числа  $b$  к  $a$  нет необходимости вычислять отдельные части суммы  $\varphi(a, b)$ , а достаточно только знать, сколько среди них имеется нечетных, то наше правило может быть представлено и так.

Пусть, как и выше,  $a = \beta b + c$ ,  $b = \gamma c + d$ ,  $c = \delta d + e \dots$ , до тех пор, пока в ряду чисел  $a, b, c, d, e, \dots$  не получится единица. Положим  $\left[\frac{1}{2}a\right] = a'$ ,  $\left[\frac{1}{2}b\right] = b'$ ,  $\left[\frac{1}{2}c\right] = c', \dots$ , и пусть  $\mu$  обозначает количество тех нечетных чисел в ряду  $a', b', c', \dots$ , за которыми непосредственно следует также нечетное число; далее, пусть  $\nu$  обозначает количество таких нечетных чисел в ряду  $\beta, \gamma, \delta, \dots$ , которым в ряду  $b', c', d', \dots$  соответствуют числа вида  $4n + 1$  или вида  $4n + 2$ . Тогда  $b$  будет квадратичным вычетом или невычетом по модулю  $a$  в зависимости от того, четно число  $\mu + \nu$  или нечетно, за исключением единственного случая, когда одновременно  $b$  четно и  $a$  имеет вид  $8n + 3$  или  $8n + 5$ ; в этом случае следует применять противоположное правило.

В нашем примере ряд  $a', b', c', d', \dots$  дает две пары следующих одно за другим нечетных чисел, так что  $\mu = 2$ ; в ряду же  $\beta, \gamma, \delta, \epsilon$ , хотя и имеются два нечетных числа, но им в ряду  $b', c', d', e'$  соответствуют числа вида  $4n + 3$ , так что  $\nu = 0$ . Поэтому число  $\mu + \nu$  будет четным, и, значит, 103 является квадратичным вычетом по модулю 379.

---

# ТЕОРИЯ БИКВАДРАТИЧНЫХ ВЫЧЕТОВ

## Сочинение первое

(*Commentationes soc. reg. sc. Götting recentiores.*, Vol. VI, Gottingae, 1828)

### 1

Теория квадратичных вычетов может быть сведена к небольшому числу основных теорем, относящихся к прекраснейшим жемчужинам высшей арифметики, которые, как мы знаем, сначала легко получались индуктивным путем, а затем были доказаны различными способами, так что в этом отношении не остается уже желать ничего лучшего.

Намного труднее, однако, теория кубических и биквадратичных вычетов. После того как мы начали исследовать эти вопросы в 1805 г., у нас, помимо очевидных элементарных предложений, получились также некоторые специальные теоремы, которые весьма замечательны как простотой формулировок, так и трудностью доказательства; однако мы скоро пришли к убеждению, что применявшиеся до сих пор арифметические принципы ни в коем случае не достаточны для обоснования общей теории, а что эта теория с необходимостью требует в некотором смысле бесконечно расширить область высшей арифметики; а как это следует понимать, будет показано в процессе настоящих исследований. Как только мы вступаем в эту новую область, тотчас же обнаруживается подход к индуктивному нахождению весьма простых и исчерпывающих всю теорию теорем; однако доказательства их скрыты столь глубоко, что их удалось извлечь на свет только после многих бесплодных попыток.

Приступая теперь к опубликованию этих исследований, мы начинаем с теории биквадратичных вычетов, причем в этом первом сочинении изложим те результаты, которые еще могут быть получены без расширения области арифметики, но которые в известном смысле пролагают к нему путь, и одновременно приводят к новым фактам в теории деления круга.

## 2

Понятие биквадратичного вычета мы ввели в п. 115 «Арифметических исследований»: именно, целое положительное или отрицательное число  $a$  называется биквадратичным вычетом целого числа  $p$ , если  $a$  сравнимо по модулю  $p$  с некоторым биквадратом, и биквадратичным невычетом, если такое сравнение невозможно. Во всех дальнейших исследованиях, когда не будет оговорено противное, будет предполагаться, что модуль  $p$  является (нечетным положительным) простым числом, и  $a$  не делится на  $p$ , ибо все остальные случаи легко могут быть сведены к этому.

## 3

Очевидно, что каждый биквадратичный вычет числа  $p$  будет также и его квадратичным вычетом, а потому каждый квадратичный невычет — также и биквадратичным невычетом. Эту теорему можно и обратить, если  $p$  является простым числом вида  $4n + 3$ . Действительно, если в этом случае  $a$  является квадратичным вычетом числа  $p$ , то положим  $a \equiv b^2 \pmod{p}$ , где  $b$  будет или квадратичным вычетом, или квадратичным невычетом. В первом случае положим  $b \equiv c^2$ , так что  $a \equiv c^4$ , т. е.  $a$  будет биквадратичным вычетом числа  $p$ ; во втором случае число  $-b$  будет квадратичным вычетом числа  $p$  (так как  $-1$  является невычетом каждого простого числа вида  $4n + 3$ ), и если положить  $-b \equiv c^2$ , то, как и раньше, будет  $a \equiv c^4$ , т. е.  $a$  будет биквадратичным вычетом числа  $p$ . Одновременно легко видеть, что других решений сравнения  $x^4 \equiv a \pmod{p}$ , кроме  $x = c$  и  $x = -c$ , в этом случае нет.

Так как эти очевидные теоремы исчерпывают всю теорию биквадратичных вычетов для простых модулей вида  $4n + 3$ , мы полностью исключаем такие модули из нашего исследования, т. е. ограничим его простыми модулями вида  $4n + 1$ .

## 4

Если  $p$  является, таким образом, простым числом вида  $4n + 1$ , то теорему предыдущего пункта обратить нельзя; действительно, могут существовать квадратичные вычеты, которые не являются одновременно биквадратичными вычетами, причем это имеет место в том случае, когда квадратичный вычет сравним с квадратом квадратичного невычета. Действительно, если положить  $a \equiv b^2$ , где  $b$  является квадратичным невычетом числа  $p$ , то если бы сравнение  $x^4 \equiv a$  удовлетворялось некоторым значением  $x \equiv c$ , имело бы место  $c^4 \equiv b^2$ , т. е. произведение  $(c^2 - b)(c^2 + b)$  делилось бы на  $p$ , вследствие чего  $p$  входило бы делителем или в сомножитель  $c^2 - b$ , или в сомножитель  $c^2 + b$ , т. е. или  $+b$ , или  $-b$  было бы квадратичным вычетом числа  $p$ , а потому они оба были бы квадратичными вычетами (так как  $-1$  является квадратичным вычетом), что противоречит нашему предположению.

Таким образом, все не делящиеся на  $p$  целые числа могут быть разбиты на три класса, первый из которых содержит биквадратичные вычеты, второй — те биквадратичные невычеты, которые одновременно являются квадратичными вычетами, и третий — квадратичные невычеты. Очевидно, что достаточно произвести такое разбиение на классы только для чисел  $1, 2, 3, \dots, p-1$ , из которых половина будет принадлежать третьему классу, а другая половина распределится по первому и второму классам.

## 5

Лучше, однако, определить четыре класса, природа которых состоит в следующем.

Пусть  $A$  — совокупность всех лежащих между  $1$  и  $p-1$  (включительно) биквадратичных вычетов, и  $e$  — произвольный квадратичный



невычет числа  $p$ . Пусть, далее,  $B$  — совокупность всех наименьших положительных вычетов по модулю  $p$ , получающихся из произведений  $eA$ , а  $C$  и  $D$  — соответственно совокупности наименьших положительных вычетов по модулю  $p$ , получающихся из произведений  $e^2A$ ,  $e^3A$ . Тогда легко видеть, что отдельные числа из  $B$  различны между собой, так же как и отдельные числа из  $C$  и отдельные числа из  $D$ , и что среди всех этих чисел не может встретиться нуль. Далее, ясно, что все числа, содержащиеся в  $A$  и  $C$ , являются квадратичными вычетами числа  $p$ , а все числа, содержащиеся в  $B$  и  $D$  — квадратичными невычетами, так что совокупности  $A$  и  $C$  заведомо не могут иметь общих чисел с совокупностями  $B$  и  $D$ . Но также не могут иметь общих чисел ни  $A$  с  $C$ , ни  $B$  с  $D$ .

I. Действительно, если мы предположим, что какое-нибудь число из  $A$ , например, число  $a$ , встречается также и в  $C$ ; далее, что оно получается из сравнимого с ним произведения  $e^2a'$ , где  $a'$  — некоторое число из совокупности  $A$ ; наконец, что  $a \equiv \alpha^4$ ,  $a' \equiv \alpha'^4$ , и целое число  $\Theta$  таково, что  $\Theta\alpha' \equiv 1$ , то  $e^2\alpha'^4 \equiv \alpha^4$ , и потому, умножив это сравнение на  $\Theta^4$ , мы получим

$$e^2 \equiv \alpha^4\Theta^4,$$

т. е.  $e^2$  будет биквадратичным вычетом, и следовательно,  $e$  — квадратичным вычетом, что противоречит предположению.

II. Точно так же, если мы предположим, что у совокупностей  $B$ ,  $D$  есть какое-нибудь общее число, которое получается из некоторых произведений  $ea$ ,  $e^3a'$ , где  $a$  и  $a'$  являются числами из совокупности  $A$ , то из сравнения  $ea \equiv e^3a'$  будет следовать  $a \equiv e^2a'$ , т. е. найдется число, которое, будучи сравнимо с произведением  $e^2a'$ , принадлежит совокупности  $C$ , и одновременно принадлежит совокупности  $A$ , что, как мы только что доказали, невозможно.

Далее, легко доказать, что все лежащие между 1 и  $p-1$  включительно квадратичные вычеты числа  $p$  обязательно должны встречаться или в  $A$ , или в  $C$ , а все лежащие в этих же границах квадратичные невычеты числа  $p$  — или в  $B$ , или в  $D$ . Действительно,

I) каждый квадратичный вычет, являющийся одновременно биквадратичным вычетом числа  $p$ , по предположению находится в  $A$ ;

II) квадратичный вычет  $h$  (меньший чем  $p$ ), который одновременно является биквадратичным невычетом, положим  $\equiv g^2$ , где  $g$  будет квадратичным невычетом. Если мы подберем такое целое число  $\gamma$ , что  $e\gamma \equiv g$ , то  $\gamma$  будет квадратичным вычетом числа  $p$ , который мы положим  $\equiv k^2$ . Тогда

$$h \equiv g^2 \equiv e^2 \gamma^2 \equiv e^2 k^4.$$

Но так как наименьший вычет числа  $k^4$  входит в  $A$ , то число  $h$ , которое получается из произведения этого числа на  $e^2$ , обязательно должно содержаться в  $C$ ;

III) если  $h$  обозначает лежащий между границами 1 и  $p-1$  квадратичный невычет числа  $p$ , и между теми же границами взято такое целое число  $g$ , что  $eg \equiv h$ , то  $g$  будет квадратичным вычетом и потому будет содержаться или в  $A$ , или в  $C$ . В первом случае  $h$ , очевидно, находится среди чисел совокупности  $B$ , а во втором — среди чисел совокупности  $D$ .

Из всего этого следует, что все числа  $1, 2, 3, \dots, p-1$  так разбиваются на четыре совокупности  $A, B, C, D$ , что каждое из этих чисел встречается в одной и только одной из этих совокупностей, и каждая совокупность содержит  $(p-1)/4$  чисел. При этой классификации классы  $A$  и  $C$  определяются однозначно, в то время как классы  $B$  и  $D$  могут изменяться, поскольку они зависят от выбора числа  $e$ , которое само всегда причисляется к классу  $B$ ; если же вместо  $e$  взять какое-нибудь другое число из класса  $D$ , то классы  $B$  и  $D$  поменяются местами.

## 6

Так как  $-1$  является квадратичным вычетом числа  $p$ , то можно положить  $-1 \equiv f^2 \pmod{p}$ , так что четырьмя корнями сравнения  $x^4 \equiv 1$  будут  $1, f, -1, -f$ . Если поэтому  $a$  является биквадратичным вычетом числа  $p$ , например,  $a \equiv \alpha^4$ , то четырьмя корнями сравнения  $x^4 \equiv a$  будут  $\alpha, f\alpha, -\alpha, -f\alpha$ , и легко видеть, что они между собой несравнимы. Отсюда вытекает, что если собрать наименьшие положительные вычеты биквадратов  $1, 16, 81, 256, \dots, (p-1)^4$ , то среди них каждый будет повторяться по четыре раза, так что

имеется  $(p-1)/4$  различных биквадратичных вычетов, которые образуют совокупность  $A$ . Если собрать наименьшие вычеты биквадратов только до  $\left(\frac{p-1}{2}\right)^4$ , то каждый будет встречаться только по два раза.

## 7

Произведение двух биквадратичных вычетов, очевидно, тоже будет биквадратичным вычетом, т. е. при перемножении двух чисел из класса  $A$  всегда получается произведение, наименьший положительный вычет которого принадлежит этому же классу. Точно так же будут содержаться в  $A$  и наименьшие положительные вычеты произведения числа из  $B$  на число из  $D$ , или числа из  $C$  на число из  $C$ .

Классу  $B$  принадлежат вычеты произведений  $A \cdot B$  и  $C \cdot D$ , классу  $C$  — вычеты произведений  $A \cdot C$ ,  $B \cdot B$  и  $D \cdot D$ , наконец, классу  $D$  — вычеты произведений  $A \cdot D$  и  $B \cdot C$ .

Доказательства настолько ясны, что достаточно провести одно из них. Пусть, например,  $s$  и  $d$  — числа из  $C$  и  $D$ , и пусть  $s \equiv e^2 a$ ,  $d \equiv e^3 a'$ , где  $a, a'$  обозначают числа из  $A$ . Тогда  $e^4 aa'$  будет биквадратичным вычетом, т. е. наименьший вычет этого числа принадлежит классу  $A$ ; а так как для произведения  $sd$  имеет место  $sd \equiv ee^4 aa'$ , его наименьший вычет будет, следовательно, содержаться в  $B$ .

Одновременно легко можно узнавать, какому классу принадлежит произведение любого числа сомножителей. Именно, если придать классам  $A, B, C, D$  соответственно характер 0, 1, 2, 3, то характер произведения будет равен или сумме характеров отдельных сомножителей, или наименьшему вычету этой суммы по модулю 4.

## 8

Не стоит тратить труда на то, чтобы доказать эти элементарные теоремы без помощи теории степенных вычетов, так как при ее помощи все может быть доказано намного легче.

Пусть  $g$  — первообразный корень по модулю  $p$ , т. е. число с тем свойством, что в ряду степеней  $g, g^2, g^3, \dots$  ни одна ранее степени

$g^{p-1}$  не сравнима с единицей по модулю  $p$ . Тогда наименьшие положительные вычеты чисел  $1, g, g^2, g^3, \dots, g^{p-2}$  с точностью до порядка расположения будут совпадать с числами  $1, 2, 3, \dots, p-1$  и будут разбиваться на четыре класса следующим образом. Будут принадлежать

| к классу | наименьшие вычеты чисел                    |
|----------|--------------------------------------------|
| $A$      | $1, g^4, g^8, g^{12}, \dots, g^{p-5}$      |
| $B$      | $g, g^5, g^9, g^{13}, \dots, g^{p-4}$      |
| $C$      | $g^2, g^6, g^{10}, g^{14}, \dots, g^{p-3}$ |
| $D$      | $g^3, g^7, g^{11}, g^{15}, \dots, g^{p-2}$ |

Отсюда немедленно получаются все предыдущие теоремы.

Точно так же, как здесь, мы разбивали на четыре класса, обозначенные нами через  $A, B, C, D$ , числа  $1, 2, 3, \dots, p-1$ , можно и любое не делящееся на  $p$  целое число причислять к одному из этих классов, в зависимости от того, каков его наименьший вычет по модулю  $p$ .

## 9

Если мы обозначим через  $f$  наименьший вычет степени  $g^{(p-1)/4}$  по модулю  $p$ , то так как  $f^2 \equiv g^{(p-1)/2} \equiv -1$  («Арифметические исследования», п. 62), буква  $f$  будет иметь здесь то же самое значение, что и в п. 6. Степень  $g^{\lambda(p-1)/4}$ , где  $\lambda$  обозначает целое положительное число, будет, таким образом, сравнима по модулю  $p$  с одним из чисел  $1, f, -1, -f$ , в зависимости от того, имеет ли  $\lambda$  соответственно вид  $4m, 4m+1, 4m+2, 4m+3$ , или, в зависимости от того, принадлежит ли наименьший вычет числа  $g^{\lambda}$  соответственно классу  $A, B, C, D$ . Отсюда мы получаем очень простой критерий для того, чтобы узнавать, к какому классу следует причислить заданное не делящееся на  $p$  число  $h$ ; именно  $h$  будет принадлежать к  $A, B, C$  или  $D$  в зависимости от того, сравнима ли степень  $h^{(p-1)/4}$  по модулю  $p$  с числом  $1, f, -1$  или  $-f$ .

В качестве следствия отсюда вытекает, что  $-1$  всегда принадлежит классу  $A$ , если  $p$  имеет вид  $8n + 1$ , и, напротив, принадлежит классу  $C$ , если  $p$  имеет вид  $8n + 3$ . Независящее от теории степенных вычетов доказательство этой теоремы легко можно провести при помощи рассуждений из п. 115, III «Арифметических исследований».

## 10

Так как все первообразные корни по модулю  $p$  получаются из вычетов степеней  $g^\lambda$ , когда  $\lambda$  принимает все значения, взаимно простые с  $p - 1$ , то легко видеть, что первообразные корни будут распределяться по совокупностям  $B$  и  $D$  равномерно, если основание  $g$  все время содержится в  $B$ . Если вместо числа  $g$  взять другой первообразный корень из совокупности  $B$ , то классификация останется прежней; если же взять за основание первообразный корень из совокупности  $D$ , то классы  $B$  и  $D$  поменяются местами.

Если разбиение на классы произведено в соответствии с указанным в предыдущем пункте критерием, то различие между классами  $B$  и  $D$  будет зависеть от того, какой из корней сравнения  $x^2 \equiv -1 \pmod{p}$  мы выбрали в качестве характеристического числа  $f$ .

## 11

Для того, чтобы легче иметь возможность пояснять примерами те более тонкие исследования, к которым мы теперь переходим, мы приведем здесь разбиение чисел на классы для всех модулей до 100. Для каждого отдельного модуля мы выбрали наименьший первообразный корень.

| $p = 5$<br>$g = 2, f = 2$ | $p = 13$<br>$g = 2, f = 8$ | $p = 17$<br>$g = 3, f = 13$ |
|---------------------------|----------------------------|-----------------------------|
| $A \mid 1$                | $A \mid 1, 3, 9$           | $A \mid 1, 4, 13, 16$       |
| $B \mid 2$                | $B \mid 2, 5, 6$           | $B \mid 3, 5, 12, 14$       |
| $C \mid 4$                | $C \mid 4, 10, 12$         | $C \mid 2, 8, 9, 15$        |
| $D \mid 3$                | $D \mid 7, 8, 11$          | $D \mid 6, 7, 10, 11$       |

$$p = 29$$

$$g = 2, f = 12$$

|     |                           |
|-----|---------------------------|
| $A$ | 1, 7, 16, 20, 23, 24, 25  |
| $B$ | 2, 3, 11, 14, 17, 19, 21  |
| $C$ | 4, 5, 6, 9, 13, 22, 28    |
| $D$ | 8, 10, 12, 15, 18, 26, 27 |

$$p = 37$$

$$g = 2, f = 31$$

|     |                                   |
|-----|-----------------------------------|
| $A$ | 1, 7, 9, 10, 12, 16, 26, 33, 34   |
| $B$ | 2, 14, 15, 18, 20, 24, 29, 31, 32 |
| $C$ | 3, 4, 11, 21, 25, 27, 28, 30, 36  |
| $D$ | 5, 6, 8, 13, 17, 19, 22, 23, 35   |

$$p = 41$$

$$g = 6, f = 32$$

|     |                                       |
|-----|---------------------------------------|
| $A$ | 1, 4, 10, 16, 18, 23, 25, 31, 37, 40  |
| $B$ | 6, 14, 15, 17, 19, 22, 24, 26, 27, 35 |
| $C$ | 2, 5, 8, 9, 20, 21, 32, 33, 36, 39    |
| $D$ | 3, 7, 11, 12, 13, 28, 29, 30, 34, 38  |

$$p = 53$$

$$g = 2, f = 30$$

|     |                                                   |
|-----|---------------------------------------------------|
| $A$ | 1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49 |
| $B$ | 2, 3, 19, 20, 26, 30, 31, 32, 35, 39, 41, 45, 48  |
| $C$ | 4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43, 52    |
| $D$ | 5, 8, 12, 14, 18, 21, 22, 23, 27, 33, 34, 50, 51  |

$$p = 61$$

$$g = 2, f = 11$$

|     |                                                          |
|-----|----------------------------------------------------------|
| $A$ | 1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58 |
| $B$ | 2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55 |
| $C$ | 3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60  |
| $D$ | 6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59 |

$p = 73$   
 $g = 5, f = 27$

|          |                                                                        |
|----------|------------------------------------------------------------------------|
| <i>A</i> | 1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72      |
| <i>B</i> | 5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68   |
| <i>C</i> | 3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70   |
| <i>D</i> | 11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62 |

$p = 89$   
 $g = 3, f = 34$

|          |                                                                                           |
|----------|-------------------------------------------------------------------------------------------|
| <i>A</i> | 1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44, 45, 50, 57, 64, 67,<br>73, 78, 81, 85, 87, 88     |
| <i>B</i> | 3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46, 48, 56, 61, 65,<br>66, 75, 77, 82, 83, 86    |
| <i>C</i> | 5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47, 49, 53, 55, 68,<br>69, 71, 72, 79, 80, 84   |
| <i>D</i> | 13, 15, 19, 26, 27, 29, 30, 31, 35, 37, 38, 51, 52, 54, 58, 59,<br>60, 62, 63, 70, 74, 76 |

$p = 97$   
 $g = 5, f = 22$

|          |                                                                                                  |
|----------|--------------------------------------------------------------------------------------------------|
| <i>A</i> | 1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47, 50, 54, 61, 62, 64,<br>73, 75, 81, 88, 91, 93, 96    |
| <i>B</i> | 5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45, 52, 56, 67, 68, 74,<br>76, 77, 78, 80, 83, 84, 92 |
| <i>C</i> | 2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48, 49, 53, 65, 66, 70,<br>72, 79, 85, 86, 89, 94, 95   |
| <i>D</i> | 7, 10, 15, 26, 28, 34, 37, 38, 39, 40, 42, 46, 51, 55, 57, 58, 59,<br>60, 63, 69, 71, 82, 87, 90 |

## 12

Так как число 2 является квадратичным вычетом всех простых чисел вида  $8n + 1$  и квадратичным невычетом всех простых чисел вида  $8n + 5$ , то для простых модулей первого вида число 2 будет содержаться в классе  $A$  или  $C$ , а для простых модулей второго вида — в классе  $B$  или  $D$ . Так как разница между классами  $B$  и  $D$  не существенна, ибо она зависит только от выбора числа  $f$ , мы оставим пока модули вида  $8n + 5$  в стороне. Если же подвергнуть модули вида  $8n + 1$  индуктивному исследованию, то мы найдем, что 2 принадлежит классу  $A$  для  $p = 73, 89, 113, 233, 257, 281, 337, 353, \dots$ , и, напротив, принадлежит классу  $C$  для  $p = 17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, \dots$

Далее, так как для простого модуля вида  $8n + 1$  число  $-1$  является биквадратичным вычетом, то очевидно, что  $-2$  всегда будет принадлежать тому же классу, что и  $+2$ .

## 13

Если сравнивать между собой примеры п. 12, то, по крайней мере на первый взгляд, кажется, что нельзя указать простой критерий для того, чтобы различать между собой модули первого вида и модули второго вида. Тем не менее имеется *два таких критерия, замечательных по изяществу и простоте*, к одному из которых приводят следующие рассуждения.

Модуль  $p$ , как простое число вида  $8n + 1$ , может быть представлен, и притом единственным образом, в виде  $a^2 + 2b^2$  («Арифметические исследования», п. 182, II); при этом мы предполагаем, что значения  $a, b$  берутся положительными. Очевидно, что  $a$  будет нечетным, а  $b$  четным; мы положим  $b = 2^{\lambda}c$ , где  $c$  уже нечетно.

I. Заметим теперь, что если  $p \equiv a^2 \pmod{c}$ , то  $p$  является квадратичным вычетом числа  $c$ , а потому и отдельных простых сомножителей, на которые  $c$  распадается; в силу же фундаментальной теоремы эти отдельные простые сомножители, в свою очередь, будут квадратичными вычетами числа  $p$ , а потому будет квадратичным вычетом числа  $p$  и их произведение  $c$ , а, следовательно, как  $b^2$ , так и  $-b^2$  будут биквадратичными вычетами.



II. Поэтому число  $-2b^2$  должно принадлежать тому же классу, что и число 2; так как  $a^2 \equiv -2b^2$ , то очевидно, что 2 будет содержаться в классе  $A$  или в классе  $C$  в зависимости от того, является ли  $a$  квадратичным вычетом или квадратичным невычетом по модулю  $p$ .

III. Предположим теперь, что  $a$  разложено на свои простые сомножители, причем те из них, которые имеют вид  $8m + 1$  или  $8m + 7$ , мы обозначим через  $\alpha, \alpha', \alpha'', \dots$ , а те, которые имеют вид  $8m + 3$  или  $8m + 5$ , — через  $\beta, \beta', \beta'', \dots$ ; количество последних пусть равно  $\mu$ . Так как  $p \equiv 2b^2 \pmod{a}$ , то  $p$  будет квадратичным вычетом тех простых сомножителей числа  $a$ , квадратичным вычетом которых является число 2, т. е. сомножителей  $\alpha, \alpha', \alpha'', \dots$ , и, напротив, квадратичным невычетом тех сомножителей, квадратичным невычетом которых является число 2, т. е. сомножителей  $\beta, \beta', \beta'', \dots$ . Поэтому, в силу фундаментальной теоремы, отдельные сомножители  $\alpha, \alpha', \alpha'', \dots$  в свою очередь будут квадратичными вычетами числа  $p$ , а отдельные сомножители  $\beta, \beta', \beta'', \dots$  — его квадратичными невычетами. Итак, мы заключаем отсюда, что произведение  $a$  является квадратичным вычетом или невычетом числа  $p$  в зависимости от того, четно  $\mu$  или нечетно.

IV. Но легко убедиться, что произведение всех  $\alpha, \alpha', \alpha'', \dots$  будет всегда иметь вид  $8m + 1$  или  $8m + 7$ , и что так же обстоит дело для произведения всех  $\beta, \beta', \beta'', \dots$ , если количество их четно, так что в этом случае и произведение  $a$  обязательно должно иметь вид  $8m + 1$  или  $8m + 7$ , и что, напротив, произведение всех  $\beta, \beta', \beta'', \dots$ , когда количество их нечетно, будет иметь вид  $8m + 3$  или  $8m + 5$ , а потому в этом случае также обстоит дело и для произведения  $a$ .

Из всего этого получается, таким образом, следующая изящная теорема.

*Если число  $a$  имеет вид  $8m + 1$  или  $8m + 7$ , то число 2 содержится в совокупности  $A$ ; если же  $a$  имеет вид  $8m + 3$  или  $8m + 5$ , то число 2 находится в совокупности  $C$ .*

Это подтверждается на примерах, приведенных в п. 11. Именно, модули первого типа разлагаются следующим образом:

$$\begin{aligned} 73 &= 1 + 2 \cdot 36, & 89 &= 81 + 2 \cdot 4, & 113 &= 81 + 2 \cdot 16, & 233 &= 225 + 2 \cdot 4. \\ 257 &= 225 + 2 \cdot 16, & 281 &= 81 + 2 \cdot 100, & 337 &= 49 + 2 \cdot 144, & 353 &= 225 + 2 \cdot 64, \end{aligned}$$

а модули второго типа — следующим образом:

$$\begin{aligned} 17 &= 9 + 2 \cdot 4, & 41 &= 9 + 2 \cdot 16, & 97 &= 25 + 2 \cdot 36, \\ 137 &= 9 + 2 \cdot 64, & 193 &= 121 + 2 \cdot 36, & 241 &= 169 + 2 \cdot 36, \\ 313 &= 25 + 2 \cdot 144, & 401 &= 9 + 2 \cdot 196, & 409 &= 121 + 2 \cdot 144, \\ 433 &= 361 + 2 \cdot 36, & 449 &= 441 + 2 \cdot 4, & 457 &= 169 + 2 \cdot 144. \end{aligned}$$

#### 14

Так как разложение числа  $p$  на простой и удвоенный квадраты имеет такую замечательную связь с вопросом о принадлежности числа 2 к тому или иному классу, то стоит потрудиться над тем, чтобы исследовать, не обещает ли подобного результата также и разложение на сумму двух квадратов, которое, как известно, тоже возможно для числа  $p$ . Мы приведем поэтому здесь разложения чисел  $p$ , для которых 2 принадлежит классам  $A$  и  $C$ .

| $A$        | $C$         |
|------------|-------------|
| $9 + 64$   | $1 + 16$    |
| $25 + 64$  | $25 + 16$   |
| $49 + 64$  | $81 + 16$   |
| $169 + 64$ | $121 + 16$  |
| $1 + 256$  | $49 + 144$  |
| $25 + 256$ | $225 + 16$  |
| $81 + 256$ | $169 + 144$ |
| $289 + 64$ | $1 + 400$   |
|            | $9 + 400$   |
|            | $289 + 144$ |
|            | $49 + 400$  |
|            | $441 + 16$  |

Прежде всего заметим, что из двух квадратов, на которые разлагается  $p$ , один, который мы обозначим через  $a^2$ , должен быть

нечетным, а другой, который мы будем обозначать через  $b^2$ , — четным. Так как  $a^2$  имеет вид  $8n + 1$ , то очевидно, что значения  $b$ , делящиеся на 2, но не делящиеся на 4, будут соответствовать значениям  $p$  вида  $8n + 5$ , которые из нашего рассмотрения пока что исключены, так как для них число 2 содержится в классе  $B$  или  $D$ . А для значений числа  $p$ , имеющих вид  $8n + 1$ , число  $b$  должно делиться на 4, и если верить нашему индуктивному заключению, к которому приводит данная нами схема, то число 2 будет принадлежать классу  $A$  для всех модулей, для которых  $b$  имеет вид  $8n$ , и классу  $C$  для всех модулей, для которых  $b$  имеет вид  $8n + 4$ . Однако эта теорема требует гораздо более глубокого исследования, чем те, которые мы производили в предыдущей главе, и доказательству ее должны быть предпосланы многие подготовительные рассуждения, касающиеся порядка, в котором следуют одно за другим числа совокупностей  $A, B, C, D$ .

## 15

Обозначим количество чисел из совокупности  $A$ , за которыми непосредственно следует число из совокупности  $A, B, C, D$ , соответственно через (00), (01), (02), (03). Точно так же количество чисел из совокупности  $B$ , за которыми непосредственно следует число из совокупности  $A, B, C, D$ , обозначим соответственно через (10), (11), (12), (13); аналогично, пусть в совокупности  $C$  имеется (20), (21), (22), (23) чисел, а в совокупности  $D$  имеется (30), (31), (32), (33) чисел, непосредственно за которыми следует число соответственно из совокупности  $A, B, C, D$ . Мы ставим себе задачу определить *a priori* эти шестнадцать количеств. Для того чтобы читателю было удобнее проверять на примерах общие выводы, мы считаем целесообразным привести здесь численные значения членов схемы

|     |       |       |       |      |
|-----|-------|-------|-------|------|
|     | (00), | (01), | (02), | (03) |
| (S) | (10), | (11), | (12), | (13) |
|     | (20), | (21), | (22), | (23) |
|     | (30), | (31), | (32), | (33) |

для отдельных модулей, для которых выше, в п. 11, мы указали распределение чисел по классам.

| $p = 5$    | $p = 13$   | $p = 17$   | $p = 29$   |
|------------|------------|------------|------------|
| 0, 1, 0, 0 | 0, 1, 2, 0 | 0, 2, 1, 0 | 2, 3, 0, 2 |
| 0, 0, 0, 1 | 1, 1, 0, 1 | 2, 0, 1, 1 | 1, 1, 2, 3 |
| 0, 0, 0, 0 | 0, 1, 0, 1 | 1, 1, 1, 1 | 2, 1, 2, 1 |
| 0, 0, 1, 0 | 1, 0, 1, 1 | 0, 1, 1, 2 | 1, 2, 3, 1 |
| $p = 37$   | $p = 41$   | $p = 53$   | $p = 61$   |
| 2, 1, 2, 4 | 0, 4, 3, 2 | 2, 3, 6, 2 | 4, 3, 2, 6 |
| 2, 2, 4, 1 | 4, 2, 2, 2 | 4, 4, 2, 3 | 3, 3, 6, 3 |
| 2, 2, 2, 2 | 3, 2, 3, 2 | 2, 4, 2, 4 | 4, 3, 4, 3 |
| 2, 4, 1, 2 | 2, 2, 2, 4 | 4, 2, 3, 4 | 3, 6, 3, 3 |
| $p = 73$   | $p = 89$   | $p = 97$   |            |
| 5, 6, 4, 2 | 3, 8, 6, 4 | 2, 6, 7, 8 |            |
| 6, 2, 5, 5 | 8, 4, 5, 5 | 6, 8, 5, 5 |            |
| 4, 5, 4, 5 | 6, 5, 6, 5 | 7, 5, 7, 5 |            |
| 2, 5, 5, 6 | 4, 5, 5, 8 | 8, 5, 5, 6 |            |

Так как модули вида  $8n + 1$  и вида  $8n + 5$  ведут себя по разному, мы должны рассматривать их отдельно; мы начнем с первых.

## 16

Число (00) показывает, сколькими различными способами может быть удовлетворено уравнение  $\alpha + 1 = \alpha'$ , где  $\alpha, \alpha'$  обозначают произвольные числа из совокупности  $A$ . Так как для модуля вида  $8n + 1$ , каковым мы его здесь предполагаем, числа  $\alpha'$  и  $p - \alpha'$  принадлежат одной и той же совокупности, то мы будем говорить короче, что (00) выражает количество различных способов, которыми можно удовлетворить уравнению  $1 + \alpha + \alpha' = p$ . Очевидно, что вместо этого уравнения может фигурировать также сравнение  $1 + \alpha + \alpha' \equiv 0 \pmod{p}$ .

Точно так же

- (01) указывает количество решений сравнения  $1 + \alpha + \beta \equiv 0 \pmod{p}$   
 (02)       »               »               »               »        $1 + \alpha + \gamma \equiv 0$   
 (03)       »               »               »               »        $1 + \alpha + \delta \equiv 0$   
 (11)       »               »               »               »        $1 + \beta + \beta' \equiv 0$

и т. д.,

где через  $\beta$  и  $\beta'$  обозначены произвольные числа из совокупности  $B$ , через  $\gamma$  — числа из совокупности  $C$ , через  $\delta$  — числа из совокупности  $D$ . Отсюда тотчас же получаются следующие шесть равенств:

$$(01) = (10), (02) = (20), (03) = (30), (12) = (21), (13) = (31), (23) = (32).$$

Из каждого решения сравнения  $1 + \alpha + \beta \equiv 0$  получается решение сравнения  $1 + \delta + \delta' \equiv 0$ , если взять за  $\delta$  то число между границами 1 и  $p-1$ , для которого  $\beta\delta \equiv 1$  (оно, очевидно, будет из совокупности  $D$ ), а за  $\delta'$  — наименьший положительный вычет произведения  $\alpha\delta$  (который тоже будет из совокупности  $D$ ); точно так же мы, очевидно, от заданного решения сравнения  $1 + \delta + \delta' \equiv 0$  возвращаемся к решению сравнения  $1 + \alpha + \beta \equiv 0$ , если выберем  $\beta$  так, что  $\beta\delta \equiv 1$ , и одновременно положим  $\alpha \equiv \beta\delta'$ . Отсюда мы заключаем, что оба сравнения имеют одинаковое число решений, т. е. что  $(01) = (33)$ .

Аналогичным образом из сравнения  $1 + \alpha + \gamma \equiv 0$  мы получаем сравнение  $\gamma' + \gamma'' + 1 \equiv 0$ , если выберем  $\gamma'$  из совокупности  $C$  так, что  $\gamma\gamma' \equiv 1$ , а за  $\gamma''$  возьмем число из этой же совокупности, сравнимое с произведением  $\alpha\gamma'$ . Из этого мы легко заключаем, что оба эти сравнения имеют одинаковое число решений, т. е. что  $(02) = (22)$ .

Точно так же из сравнения  $1 + \alpha + \delta \equiv 0$  мы выводим сравнение  $\beta + \beta' + 1 \equiv 0$ , выбирая  $\beta, \beta'$  так, что  $\beta\delta \equiv 1$  и  $\beta\alpha \equiv \beta'$ , и потому  $(03) = (11)$ .

Наконец, из сравнения  $1 + \beta + \gamma \equiv 0$  мы аналогичным образом выводим как сравнение  $\delta + 1 + \beta' \equiv 0$ , так и сравнение  $\gamma' + \delta' + 1 \equiv 0$ , и заключаем отсюда, что  $(12) = (13) = (23)$ .

Мы имеем, следовательно, одиннадцать уравнений, связывающих наши шестнадцать неизвестных величин, так что они могут быть сведены к пяти, и схема  $(S)$  представляется следующим образом:

$$\begin{array}{cccc} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i. \end{array}$$

Но легко можно присоединить еще три новых уравнения. Именно, так как за каждым числом из совокупности  $A$ , за исключением последнего числа  $p-1$ , должно следовать число из какой-нибудь из совокупностей  $A$ ,  $B$ ,  $C$  или  $D$ , то мы имеем

$$(00) + (01) + (02) + (03) = 2n - 1,$$

и точно так же

$$(10) + (11) + (12) + (13) = 2n,$$

$$(20) + (21) + (22) + (23) = 2n,$$

$$(30) + (31) + (32) + (33) = 2n.$$

Во введенных обозначениях первые три равенства дают

$$h + i + k + l = 2n - 1,$$

$$i + l + 2m = 2n$$

$$k + m = n.$$

Четвертое уравнение будет совпадать со вторым. При помощи этих уравнений можно исключить три неизвестных, благодаря чему шестнадцать неизвестных уже сводятся к двум.

## 17

Для того, чтобы достигнуть полного решения, мы хотим сейчас найти число решений сравнения

$$1 + \alpha + \beta + \gamma \equiv (\text{mod } p),$$

где  $\alpha$ ,  $\beta$ ,  $\gamma$  обозначают произвольные числа из совокупностей  $A$ ,  $B$ ,  $C$ . Очевидно, что значение  $\alpha = p-1$  невозможно, так как не может быть  $\beta + \gamma \equiv 0$ ; если же вместо  $\alpha$  подставлять по порядку остальные значения, то  $h$ ,  $i$ ,  $k$ ,  $l$  будут принадлежащими соответственно к  $A$ ,  $B$ ,  $C$ ,  $D$  значениями выражения  $1 + \alpha$ . Но для каждого данного принадлежащего совокупности  $A$  значения выражения

$1 + \alpha$ , например, для  $1 + \alpha = \alpha^\circ$ , сравнение  $\alpha^\circ + \beta + \gamma \equiv 0$  обладает столькими же решениями, что и сравнение  $1 + \beta' + \gamma' \equiv 0$  (именно, если положить  $\beta \equiv \alpha^\circ \beta'$ ,  $\gamma \equiv \alpha^\circ \gamma'$ ), т. е.  $(12) = m$  решениями. Точно так же для каждого данного значения выражения  $1 + \alpha$ , принадлежащего совокупности  $B$ , например, для  $1 + \alpha = \beta^\circ$ , сравнение  $\beta^\circ + \beta + \gamma \equiv 0$  имеет столько же решений, что и сравнение  $1 + \alpha' + \beta' \equiv 0$  (именно, если положить  $\beta \equiv \beta^\circ \alpha'$ ,  $\gamma \equiv \beta^\circ \beta'$ ), т. е.  $(01) = i$  решений. Аналогично, для каждого данного принадлежащего совокупности  $C$  значения выражения  $1 + \alpha$ , например, для  $1 + \alpha = \gamma^\circ$ , сравнение  $\gamma^\circ + \beta + \gamma \equiv 0$  разрешимо столькими же различными способами, что и сравнение  $1 + \delta + \alpha' \equiv 0$  (именно, если положить  $\beta \equiv \gamma^\circ \delta$ ,  $\gamma \equiv \gamma^\circ \alpha'$ ), т. е. число решений будет равно  $(03) = l$ . Наконец, для каждого данного значения выражения  $1 + \alpha$ , принадлежащего совокупности  $D$ , например, для  $1 + \alpha = \delta^\circ$ , сравнение  $\delta^\circ + \beta + \gamma \equiv 0$  обладает столькими же решениями, что и сравнение  $1 + \gamma' + \delta' \equiv 0$  (именно, если положить  $\beta \equiv \delta^\circ \gamma'$ ,  $\gamma \equiv \delta^\circ \delta'$ ), т. е.  $(23) = m$  решениями. Таким образом, если мы соберем все эти решения, то получим, что сравнение  $1 + \alpha + \beta + \gamma \equiv 0$  имеет

$$hm + i^2 + kl + lm$$

различных решений.

Но совершенно аналогичным образом выводится, что если за  $\beta$  брать по порядку отдельные числа из совокупности  $B$ , то сумма  $1 + \beta$  будет принимать  $(10) = i$ ,  $(11) = l$ ,  $(12) = m$ ,  $(13) = m$  значений, принадлежащих соответственно совокупностям  $A$ ,  $B$ ,  $C$ ,  $D$ , и что для каждого данного значения выражения  $1 + \beta$  сравнение  $1 + \beta + \alpha + \gamma \equiv 0$  будет иметь  $(02) = k$ ,  $(31) = m$ ,  $(20) = k$ ,  $(13) = m$  решений, в зависимости от того, в какой из совокупностей  $A$ ,  $B$ ,  $C$ ,  $D$  находится  $1 + \beta$ ; таким образом, число всех решений будет равно

$$ik + lm + km + m^2.$$

К этому же значению мы придем, если будем основывать подсчет на рассмотрении значений суммы  $1 + \gamma$ .

Из этих двух выражений для одного и того же числа мы получаем уравнение

$$0 = hm + i^2 + kl - ik - km - m^2,$$

откуда, исключая  $h$  при помощи уравнения  $h = 2m - k - 1$ , находим

$$0 = (k - m)^2 + i^2 + kl - ik - k^2 - m.$$

Но два последних уравнения из п. 16 дают  $k = \frac{1}{2}(l + i)$ , и если подставить это значение, то  $i^2 + kl - ik - k^2$  перейдет в  $\frac{1}{4}(l - 1)^2$ , а потому предыдущее уравнение, после умножения его на 4, перейдет в следующее:

$$0 = 4(k - m)^2 + (l - i)^2 - 4m.$$

Так как  $4m = 2(k + m) - 2(k - m) = 2n - 2(k - m)$ , отсюда следует, что

$$2n = 4(k - m)^2 + 2(k - m) + (l - i)^2,$$

или

$$8n + 1 = [4(k - m) + 1]^2 + 4(l - i)^2.$$

Если поэтому положить

$$4(k - m) + 1 = a, \quad 2l - 2i = b,$$

то мы получаем

$$p = a^2 + b^2.$$

Но, как известно,  $p$  может быть разложено на два квадрата только одним единственным способом, причем из этих квадратов нечетный должен быть взят за  $a^2$ , а четный — за  $b^2$ , так что  $a^2$  и  $b^2$  являются вполне определенными числами. Но и само  $a$  будет вполне определенным числом; действительно, основание квадрата должно быть взято положительным или отрицательным в зависимости от того, имеет ли положительное основание вид  $4M + 1$  или  $4M + 3$ . Об определении знака числа  $b$  мы будем сейчас говорить.

Если скомбинировать теперь эти новые уравнения с последними тремя уравнениями из п. 16, то пять чисел  $h, i, k, l, m$  будут



однозначно определяться через  $a$ ,  $b$ ,  $n$  следующим образом:

$$\begin{aligned} 8h &= 4n - 3a - 5, \\ 8i &= 4n + a - 2b - 1, \\ 8k &= 4n + a - 1, \\ 8l &= 4n + a + 2b - 1, \\ 8m &= 4n - a + 1. \end{aligned}$$

Если вместо  $n$  желательно ввести модуль  $p$ , то схема (S), после умножения отдельных ее членов на 16, чтобы избавить их от дробей, будет выглядеть следующим образом:

$$\begin{array}{c|c|c|c} p - 6a - 11 & p + 2a - 4b - 3 & p + 2a - 3 & p + 2a + 4b - 3 \\ p - 2a - 4b - 3 & p + 2a + 4b - 3 & p - 2a + 1 & p - 2a + 1 \\ p + 2a - 3 & p - 2a + 1 & p + 2a - 3 & p - 2a + 1 \\ p + 2a + 4b - 3 & p - 2a + 1 & p - 2a + 1 & p + 2a - 4b - 3. \end{array}$$

19

Остается только еще показать, как может быть определен знак числа  $b$ . Выше, в п. 10, мы уже отмечали, что различие между совокупностями  $B$  и  $D$  само по себе несущественно, а зависит от выбора числа  $f$ , за которое нужно брать один из корней сравнения  $x^2 \equiv -1$ , и что эти совокупности меняются местами, если вместо одного корня взять другой. Но так как вид приведенной выше схемы показывает, что подобная перестановка совокупностей равносильна изменению знака у  $b$ , то можно предвидеть, что должна существовать связь между знаком числа  $b$  и числом  $f$ . Чтобы выяснить ее, заметим прежде всего, что если обозначить через  $\mu$  целое неотрицательное число и заставить  $z$  пробегать все числа  $1, 2, 3, \dots, p-1$ , то по модулю  $p$  будет либо  $\sum z^\mu \equiv 0$ , если  $\mu$  не делится на  $p-1$ , либо  $\sum z^\mu \equiv -1$ , если  $\mu$  делится на  $p-1$ . Вторая часть теоремы вытекает из того, что для каждого делящегося на  $p-1$  значения  $\mu$  имеет место  $z^\mu \equiv 1$ ; первую же часть мы докажем следующим образом. Если  $g$  обозначает первообразный корень, то совокупность всех значений  $z$  будет совпадать с совокупностью наименьших вычетов всевозможных чисел  $g^y$ , когда  $y$

принимает все значения  $0, 1, 2, 3, \dots, p-2$ , и потому  $\sum z^\mu \equiv \sum g^{\mu\gamma}$ . Но

$$\sum g^{\mu\gamma} \equiv \frac{g^{\mu(p-1)} - 1}{g^\mu - 1},$$

и потому

$$(g^\mu - 1) \sum z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0.$$

А так как для не делящегося на  $p-1$  значения  $\mu$  число  $g^\mu$  не сравнимо с 1, т. е.  $g^\mu - 1$  не делится на  $p$ , то отсюда следует, что  $\sum z^\mu \equiv 0$ .

Если теперь разложить степень  $(z^4 + 1)^{(p-1)/4}$  по формуле бинома, то, в силу предпосланной леммы будет выполняться сравнение

$$\sum (z^4 + 1)^{(p-1)/4} \equiv -2 \pmod{p}.$$

Но наименьшие вычеты всевозможных  $z^4$  представляют все числа совокупности  $A$ , причем каждое из них встречается по четыре раза; поэтому среди наименьших вычетов чисел  $z^4 + 1$  мы имеем

|         |                            |      |
|---------|----------------------------|------|
| $4(00)$ | принадлежащих совокупности | $A,$ |
| $4(01)$ | »                          | $B,$ |
| $4(02)$ | »                          | $C,$ |
| $4(03)$ | »                          | $D,$ |

и четыре будут равны 0 (именно, для  $z^4 \equiv p-1$ ). Отсюда, принимая во внимание критерии совокупностей  $A, B, C, D$ , мы выводим сравнение

$$\sum (z^4 + 1)^{(p-1)/4} \equiv 4(00) + 4f(01) - 4(02) - 4f(03),$$

откуда

$$-2 \equiv 4(00) + 4f(01) - 4(02) - 4f(03),$$

или, подставляя вместо  $(00), (01), \dots$  их значения, найденные в предыдущем пункте, имеем

$$-2 \equiv -2a - 2 - 2bf.$$

Отсюда заключаем, что всегда  $a + bf \equiv 0$ , или, умножая на  $f$ , что  $b \equiv af$ ,

и это сравнение служит для определения знака числа  $b$ , когда  $f$  уже выбрано, или, если знак числа  $b$  уже предписан, то для определения числа  $f$ .

20

После того как для модулей вида  $8n + 1$  мы полностью решили нашу задачу, мы переходим к случаю, когда  $p$  имеет вид  $8n + 5$ ; теперь мы можем быть в изложении более краткими, так как все выводы лишь слегка отличаются от предыдущих.

Так как для модуля вида  $8n + 5$  число  $-1$  принадлежит классу  $C$ , то дополнения чисел из совокупностей  $A, B, C, D$  до  $p$  будут содержаться соответственно в совокупностях  $C, D, A, B$ . Отсюда легко получить, что

| знак: | обозначает количество решений сравнения: |
|-------|------------------------------------------|
| (00)  | $1 + \alpha + \gamma \equiv 0$           |
| (01)  | $1 + \alpha + \delta \equiv 0$           |
| (02)  | $1 + \alpha + \alpha' \equiv 0$          |
| (03)  | $1 + \alpha + \beta \equiv 0$            |
| (10)  | $1 + \beta + \gamma \equiv 0$            |
| (11)  | $1 + \beta + \delta \equiv 0$            |
| (12)  | $1 + \beta + \alpha \equiv 0$            |
| (13)  | $1 + \beta + \beta' \equiv 0$            |
| (20)  | $1 + \gamma + \gamma' \equiv 0$          |
| (21)  | $1 + \gamma + \delta \equiv 0$           |
| (22)  | $1 + \gamma + \alpha \equiv 0$           |
| (23)  | $1 + \gamma + \beta \equiv 0$            |
| (30)  | $1 + \delta + \gamma \equiv 0$           |
| (31)  | $1 + \delta + \delta' \equiv 0$          |
| (32)  | $1 + \delta + \alpha \equiv 0$           |
| (33)  | $1 + \delta + \beta \equiv 0,$           |

откуда тотчас же получаются шесть уравнений

$$(00) = (22), (01) = (32), (03) = (12), (10) = (23), (11) = (33), (21) = (30).$$

Если сравнение  $1 + \alpha + \gamma \equiv 0$  умножить на число  $\gamma'$  из совокупности  $C$ , которое выбрано так, что  $\gamma\gamma' \equiv 1$ , и за  $\gamma''$  взять наименьший вычет произведения  $\alpha\gamma'$ , который, очевидно, тоже принадлежит совокупности  $C$ , то получается сравнение  $\gamma' + \gamma'' + 1 \equiv 0$ , из чего мы заключаем, что  $(00) = (20)$ .

Совершенно аналогичным образом мы получаем уравнения

$$(01) = (13), (03) = (31), (10) = (11) = (21).$$

При помощи этих одиннадцати уравнений мы можем наши шестнадцать неизвестных свести к пяти и схему (S) представить в виде

$$\begin{array}{cccc} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m. \end{array}$$

Далее мы получаем уравнения

$$\begin{aligned} (00) + (01) + (02) + (03) &= 2n + 1, \\ (10) + (11) + (12) + (13) &= 2n + 1, \\ (20) + (21) + (22) + (23) &= 2n, \\ (30) + (31) + (32) + (33) &= 2n + 1, \end{aligned}$$

или, если использовать введенные выше обозначения, — следующие три уравнения:

$$(I) \quad \begin{cases} h + i + k + l = 2n + 1, \\ 2m + i + l = 2n + 1, \\ h + m = n, \end{cases}$$

при помощи которых число наших неизвестных уже может быть сведено к двум.

Остальные уравнения мы выводим из рассмотрения числа решений сравнения  $1 + \alpha + \beta + \gamma \equiv 0$  (причем и здесь мы обозначаем

через  $\alpha, \beta, \gamma$  произвольные числа соответственно из совокупностей  $A, B, C$ ). Именно, принимая сначала во внимание, что  $1 + \alpha$  дает  $h, i, k, l$  чисел соответственно из совокупностей  $A, B, C, D$ , и что для каждого данного значения  $\alpha$  в этих четырех случаях получается соответственно  $m, l, i, m$  решений, мы находим, что количество всех решений равно

$$hm + il + ik + lm.$$

Во-вторых, так как  $1 + \beta$  представляет  $m, m, l, i$  чисел, принадлежащих соответственно совокупностям  $A, B, C, D$ , и для каждого данного значения числа  $\beta$  в этих четырех случаях существует соответственно  $h, m, h, m$  решений, то число всех решений равно

$$hm + m^2 + hl + im,$$

откуда мы получаем уравнение

$$0 = m^2 + hl + im - il - ik - lm,$$

которое при помощи вытекающего из (I) равенства  $k = 2m - h$  переходит в уравнение

$$0 = m^2 + hl + hi - il - im - lm.$$

Но из уравнений (I) мы получаем также  $l + i = 1 + 2h$ ; поэтому

$$2i = 1 + 2h + (i - l),$$

$$2l = 1 + 2h - (i - l).$$

Если подставить эти значения в предыдущее уравнение, то получается

$$0 = 4m^2 - 4m - 1 - 8hm + 4h^2 + (i - l)^2.$$

Наконец, если мы теперь подставим вместо  $4m$  выражение  $2(h + m) - 2(h - m)$ , или, в силу последнего из уравнений (I), выражение  $2n - 2(h - m)$ , то мы получим

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (i - l)^2,$$

и потому

$$8n + 5 = [4(h - m) + 1]^2 + 4(i - l)^2.$$

Поэтому, если положить

$$4(h - m) + 1 = a, \quad 2i - 2l = b,$$

то будет выполняться равенство

$$p = a^2 + b^2.$$

Но так как и в этом случае  $p$  может быть только одним единственным способом разложено на два квадрата, один четный и один нечетный, то  $a^2$  и  $b^2$  будут вполне определенными числами; действительно, очевидно, что  $a^2$  должно быть положено равным нечетному, а  $b^2$  — четному квадрату. Кроме того, знак числа  $a$  определяется тем, что должно быть  $a \equiv 1 \pmod{4}$ , а знак числа  $b$  — тем, что имеет место  $b \equiv af \pmod{p}$ , что легко доказывается при помощи рассуждений, совершенно аналогичных проведенным в предыдущем пункте:

Если считать это доказанным, то пять чисел  $h, i, k, l, m$  следующим образом определяются числами  $a, b, n$ :

$$\begin{aligned} 8h &= 4n + a - 1, \\ 8i &= 4n + a + 2b + 3, \\ 8k &= 4n - 3a + 3, \\ 8l &= 4n + a - 2b + 3, \\ 8m &= 4n - a + 1, \end{aligned}$$

или, если предпочитать выражения через  $p$ , то умноженные на 16 члены схемы (S) оказываются следующими:

$$\begin{array}{c|c|c|c} p + 2a - 7 & p + 2a + 4b + 1 & p - 2a + 1 & p + 2a - 4b + 1 \\ p - 2a - 3 & p - 2a - 3 & p + 2a - 4b + 1 & p + 2a + 4b + 1 \\ p + 2a - 7 & p - 2a - 3 & p + 2a - 7 & p - 2a - 3 \\ p - 2a - 3 & p + 2a - 4b + 1 & p + 2a + 4b + 1 & p - 2a - 3 \end{array}$$

После того как мы решили нашу задачу, мы возвращаемся к основному исследованию, причем ставим себе теперь целью окончательное определение совокупности, к которой принадлежит число 2.

I. Если  $p$  имеет вид  $8n + 1$ , то как уже установлено, число 2 содержится или в совокупности  $A$ , или в совокупности  $C$ . В первом случае легко видеть, что совокупности  $A$  принадлежат также и числа  $\frac{1}{2}(p-1)$ ,  $\frac{1}{2}(p+1)$ , в то время как во втором случае они принадлежат совокупности  $C$ . Примем теперь во внимание, что если  $\alpha$  и  $\alpha + 1$  являются соседними числами совокупности  $A$ , то соседними же будут и числа  $p - \alpha - 1$ ,  $p - \alpha$ , т. е. что те числа совокупности  $A$ , за которыми следует число из этой же совокупности, могут быть сгруппированы на пары ассоциированных одно с другим (именно, ассоциированы  $\alpha$  и  $p - 1 - \alpha$ ); тогда мы убедимся, что количество (00) таких чисел будет всегда четным, если нет числа, ассоциированного с самим собой, т. е. если  $\frac{1}{2}(p-1)$  не принадлежит совокупности  $A$ , в противном же случае указанное количество нечетно. Отсюда мы заключаем, что (00) нечетно, если число 2 принадлежит совокупности  $A$ , и четно, если 2 принадлежит совокупности  $C$ . Но мы имеем

$$16(00) = a^2 + b^2 - 6a - 11,$$

или, если положить  $a = 4q + 1$ ,  $b = r$  (ср. п. 14),

$$(00) = q^2 - q + r^2 - 1.$$

Но так как  $q^2 - q$ , очевидно, всегда четно, то число (00) будет нечетным или четным в зависимости от того, четно или нечетно число  $r$ , и потому число 2 будет принадлежать совокупности  $A$  или совокупности  $C$  в зависимости от того, имеет ли  $b$  вид  $8m$  или вид  $8m + 4$ . Это и представляет собой теорему, которую мы в п. 14 нашли индуктивным путем.

II. Но и во втором случае, когда  $p$  имеет вид  $8n + 5$ , мы можем так же завершить исследование. Число 2 принадлежит здесь или к  $B$ , или к  $D$ , и легко видеть, что в первом случае число  $\frac{1}{2}(p - 1)$  принадлежит к  $B$ , а число  $\frac{1}{2}(p + 1) — к  $D$ , а во втором случае  $\frac{1}{2}(p - 1) — к  $D$ , а  $\frac{1}{2}(p + 1) — к  $B$ . Учтем теперь, что если  $\beta$  является таким числом из  $B$ , за которым следует число из  $D$ , то и число  $p - \beta - 1$  будет содержаться в  $B$ , а число  $p - \beta — в  $D$ , т. е. что всегда вместе со всяким числом, обладающим указанным свойством, этим свойством обладает и число, ассоциированное с первым. Поэтому количество таких чисел, т. е. (13), будет четным, за исключением случая, когда одно из них ассоциировано само с собой, т. е. когда  $\frac{1}{2}(p - 1)$  принадлежит совокупности  $B$ , а  $\frac{1}{2}(p + 1) — совокупности  $D$ ; в этом случае число (13) будет нечетным. Отсюда мы заключаем, что (13) четно, если число 2 принадлежит совокупности  $D$ , и, напротив, нечетно, если 2 принадлежит совокупности  $B$ . Но мы имеем$$$$$

$$16(13) = a^2 + b^2 + 2a + 4b + 1,$$

или, если положить  $a = 4q + 1$ ,  $b = 4r + 2$ ,

$$(13) = q^2 + q + r^2 + 2r + 1.$$

Поэтому число (13) будет нечетным, когда число  $r$  четно; напротив, (13) будет четным, когда  $r$  нечетно. Из этого мы заключаем, что число 2 принадлежит совокупности  $B$ , если  $b$  имеет вид  $8m + 2$ , и, напротив, принадлежит совокупности  $D$ , если  $b$  имеет вид  $8m + 6$ .

**Результат этих исследований** может быть высказан следующим образом.

Число 2 принадлежит совокупности  $A$ ,  $B$ ,  $C$  или  $D$  в зависимости от того, имеет ли число  $b/2$  вид  $4m$ ,  $4m + 1$ ,  $4m + 2$  или  $4m + 3$



## 22

В «Арифметических исследованиях» мы изложили общую теорию деления круга и решения уравнения  $x^p - 1 = 0$ , и между прочим доказали, что если  $\mu$  является делителем числа  $p - 1$ , то функция  $(x^p - 1)/(x - 1)$  при помощи вспомогательного уравнения порядка  $\mu$  может быть разложена на  $\mu$  сомножителей порядка  $(p - 1)/\mu$ . Кроме общей теории этого решения, мы в пп. 356—358 указанного сочинения отдельно рассматривали специальные случаи, когда  $\mu = 2$  или  $\mu = 3$  и показали, как в этих случаях строить вспомогательное уравнение *a priori*, т. е. без развертывания схемы наименьших вычетов степеней некоторого первообразного корня по модулю  $p$ . Теперь, хотя мы на это и не указывали, внимательные читатели могут заметить тесную связь следующего случая указанной теории, т. е. случая  $\mu = 4$ , с изложенными здесь в пп. 15—20 исследованиями, при помощи которых этот случай также может быть без труда разобран полностью. Однако мы оставим это рассмотрение до другого случая, а в настоящем сочинении предпочтем проводить исследование в чисто арифметической форме, без какой-либо связи с теорией уравнения  $x^p - 1 = 0$ . Мы в заключение рассмотрим еще несколько новых чисто арифметических теорем, которые находятся в теснейшей связи с предметом, разбиравшимся до сих пор.

## 23

Если степень  $(x^4 + 1)^{(p-1)/2}$  разложить по формуле бинома, то в разложении будет содержаться три члена, у которых показатель степени при  $x$  делится на  $p - 1$ , именно

$$x^{2(p-1)}, \quad Px^{p-1} \text{ и } 1,$$

где  $P$  обозначает средний коэффициент

$$\frac{\frac{1}{2}(p-1) \cdot \frac{1}{2}(p-3) \cdot \frac{1}{2}(p-5) \cdots \frac{1}{4}(p+3)}{1 \quad \cdot 2 \quad \cdot 3 \quad \cdots \frac{1}{4}(p-1)}.$$

Таким образом, если подставлять вместо  $x$  по порядку числа  $1, 2, 3, \dots, p-1$ , то по теореме п. 19 мы получаем

$$\sum (x^4 + 1)^{(p-1)/2} \equiv -2 - P.$$

Но если принять во внимание то, что было изложено в п. 19, и то, что числа из совокупностей  $A, B, C, D$ , возведенные в степень с показателем  $(p-1)/2$ , сравнимы по модулю  $p$  соответственно с числами  $+1, -1, +1, -1$ , то легко видеть, что

$$\sum (x^4 + 1)^{(p-1)/2} \equiv 4(00) - 4(01) + 4(02) - 4(03),$$

и потому, согласно данным в конце п. 18 и в конце п. 20 схемам,

$$\sum (x^4 + 1)^{(p-1)/2} \equiv -2a - 2.$$

Сравнение этих двух значений дает следующую очень изящную теорему.

*Имеет место*

$$P \equiv 2a \pmod{p}.$$

Если четыре произведения

$$\begin{aligned} & 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{1}{4}(p-1) \\ & \frac{1}{4}(p+3) \cdot \frac{1}{4}(p+7) \cdot \frac{1}{4}(p+11) \cdot \dots \cdot \frac{1}{2}(p-1), \\ & \frac{1}{2}(p+1) \cdot \frac{1}{2}(p+3) \cdot \frac{1}{2}(p+5) \cdot \dots \cdot \frac{3}{4}(p-1), \\ & \frac{1}{4}(3p+1) \cdot \frac{1}{4}(3p+5) \cdot \frac{1}{4}(3p+9) \cdot \dots \cdot (p-1) \end{aligned}$$

обозначить соответственно через  $q, r, s, t$ , то формулировка этой теоремы примет вид

$$2a \equiv \frac{r}{q} \pmod{p}.$$

Так как у каждого сомножителя числа  $q$  его дополнение до  $p$  входит в  $t$ , то  $q \equiv t \pmod{p}$ , если число сомножителей четно, т. е. если  $p$  имеет вид  $8n + 1$ , и  $q \equiv -t$ , если число сомножителей нечетно, т. е.  $p$  имеет вид  $8n + 5$ . Точно так же в первом случае будет выполняться сравнение  $r \equiv s$ , а во втором — сравнение  $r \equiv -s$ . В обоих случаях  $qr \equiv st$ , а так как, как известно,  $qrst \equiv -1$ , то  $q^2 r^2 \equiv -1$ , и потому  $qr \equiv \pm f \pmod{p}$ . Если связать это сравнение с только что найденной теоремой, то получается  $r^2 \equiv \pm 2af$ , и потому, согласно пп. 19, 20,

$$2b \equiv \pm r^2 \pmod{p}^*.$$

Весьма замечательно, что разложение числа  $p$  может быть найдено совершенно прямыми методами; именно, основанием нечетного квадрата будет абсолютно наименьший вычет числа  $r/2q$ , а основанием четного квадрата — абсолютно наименьший вычет числа  $r^2/2$  по модулю  $p$ . Выражение  $r/2q$ , значение которого для  $p = 5$  равно 1, для бóльших значений  $p$  может быть представлено также следующим образом:

$$\frac{6 \cdot 10 \cdot 14 \cdot 18 \dots (p-3)}{2 \cdot 3 \cdot 4 \cdot 5 \dots \frac{1}{4}(p-1)}.$$

Так как мы, кроме того, знаем, с каким знаком следует брать получающееся из этой формулы основание нечетного квадрата, а именно, с тем, при котором оно имеет вид  $8m + 1$ , то особенно достойно внимания, что для основания четного квадрата подобного общего критерия до сих пор не найдено. Если бы кто-нибудь его нашел и сообщил нам, мы были бы за это очень благодарны. Пока же я считаю полезным привести здесь значения чисел  $a$ ,  $b$ ,  $f$ , которые получаются для значений  $p$ , не превосходящих 200, из наименьших вычетов выражений  $r/2q$ ,  $r^2/2$ ,  $qr$ .

---

\* А также  $\{(a \mp b)q\}^2 \equiv a \equiv \left(\frac{r - qr^2}{2}\right)^2$ .

| $p$ | $a$ | $b$ | $f$ |
|-----|-----|-----|-----|
| 5   | + 1 | + 2 | 2   |
| 13  | — 3 | — 2 | 5   |
| 17  | + 1 | — 4 | 13  |
| 29  | + 5 | + 2 | 12  |
| 37  | + 1 | — 6 | 31  |
| 41  | + 5 | + 4 | 9   |
| 53  | — 7 | — 2 | 23  |
| 61  | + 5 | — 6 | 11  |
| 73  | — 3 | — 8 | 27  |
| 89  | + 5 | — 8 | 34  |
| 97  | + 9 | + 4 | 22  |
| 101 | + 1 | —10 | 91  |
| 109 | — 3 | +10 | 33  |
| 113 | — 7 | + 8 | 15  |
| 137 | —11 | + 4 | 37  |
| 149 | — 7 | —10 | 44  |
| 157 | —11 | — 6 | 129 |
| 173 | +13 | + 2 | 80  |
| 181 | + 9 | +10 | 162 |
| 193 | — 7 | +12 | 81  |
| 197 | + 1 | —14 | 183 |

# ТЕОРИЯ БИКВАДРАТИЧНЫХ ВЫЧЕТОВ

## Сочинение второе

*(Commentationes soc. reg. sc. Gotting.  
recentiores, Vol. VII, Gottingae, 1832)*

24

В первом сочинении было полностью изложено то, что необходимо для биквадратичной классификации числа  $+2$ . Именно, если мы будем считать все числа, не делящиеся на модуль  $p$  (который предполагается простым числом вида  $4n + 1$ ) разбитыми на четыре класса  $A, B, C, D$ , причем каждое число относится к первому, второму, третьему или четвертому классу, если его степень с показателем  $(p - 1)/4$  сравнима соответственно с  $+1, +f, -1, -f$ , где  $f$  обозначает один из двух корней сравнения  $f^2 \equiv -1 \pmod{p}$ , то ответ на вопрос, к какой совокупности принадлежит число  $+2$ , зависит от разложения числа  $p$  на два квадрата, а именно, если положить  $p = a^2 + b^2$ , где  $a^2$  обозначает нечетный, а  $b^2$  — четный квадрат, и предположить, что знаки чисел  $a, b$  выбраны так, что  $a \equiv 1 \pmod{4}$ ,  $b \equiv af \pmod{p}$ , то число  $+2$  будет принадлежать к совокупности  $A, B, C$  или  $D$  в зависимости от того, имеет ли число  $b/2$  соответственно вид  $4n, 4n + 1, 4n + 2, 4n + 3$ .

Отсюда немедленно получается также правило для классификации числа  $-2$ . Именно, так как число  $-1$  принадлежит классу  $A$  для четного значения  $b/2$ , и классу  $C$  для нечетного значения  $b/2$ , то, согласно теореме п. 7, число  $-2$  будет принадлежать классу  $A$ ,

$B$ ,  $C$  или  $D$  в зависимости от того, имеет ли число  $b/2$  соответственно вид  $4n$ ,  $4n + 3$ ,  $4n + 2$  или  $4n + 1$ . Эти теоремы могут быть также выражены следующим образом.

| Число                    | +2                              | —2   |
|--------------------------|---------------------------------|------|
| принадлежит совокупности | если $b$ по модулю 8 сравнимо с |      |
| $A$                      | 0                               | 0    |
| $B$                      | $2a$                            | $6a$ |
| $C$                      | $4a$                            | $4a$ |
| $D$                      | $6a$                            | $2a$ |

Легко убедиться, что выраженные подобным образом теоремы уже не зависят от условия  $a \equiv 1 \pmod{4}$ , а имеют силу и при  $a \equiv 3 \pmod{4}$ , если только второе условие,  $af \equiv b \pmod{p}$  сохраняется.

Точно так же легко видеть, что содержание этих теорем изящным образом может быть объединено в одну единственную формулу, именно,

если  $a$  и  $b$  берутся положительными, то всегда

$$b^{ab/2} \equiv a^{ab/2} \cdot 2^{(p-1)/4} \pmod{p}.$$

Теперь мы посмотрим, что дает индуктивное рассмотрение относительно классификации числа 3. Если таблицу п. 11 продолжить дальше (беря все время наименьший первообразный корень), то

она будет показывать, что число  $+3$  принадлежит

совокупности:

| A для |     |     | B для |     |     | C для |     |     | D для |     |     |
|-------|-----|-----|-------|-----|-----|-------|-----|-----|-------|-----|-----|
| $p$   | $a$ | $b$ | $p$   | $a$ | $b$ | $p$   | $a$ | $b$ | $p$   | $a$ | $b$ |
| 13    | — 3 | + 2 | 17    | + 1 | — 4 | 37    | + 1 | —6  | 5     | + 1 | + 2 |
| 109   | — 3 | +10 | 29    | + 5 | + 2 | 61    | + 5 | —6  | 41    | + 5 | — 4 |
| 181   | + 9 | +10 | 53    | — 7 | + 2 | 73    | — 3 | —8  | 149   | — 7 | +10 |
| 193   | — 7 | —12 | 89    | + 5 | — 8 | 97    | + 9 | +4  | 173   | +13 | + 2 |
| 229   | —15 | + 2 | 101   | + 1 | +10 | 157   | —11 | —6  |       |     |     |
| 277   | + 9 | +14 | 113   | — 7 | — 8 | 241   | —15 | —4  |       |     |     |
|       |     |     | 137   | —11 | — 4 |       |     |     |       |     |     |
|       |     |     | 197   | + 1 | —14 |       |     |     |       |     |     |
|       |     |     | 233   | +13 | + 8 |       |     |     |       |     |     |
|       |     |     | 257   | + 1 | —16 |       |     |     |       |     |     |
|       |     |     | 269   | +13 | +10 |       |     |     |       |     |     |
|       |     |     | 281   | + 5 | +16 |       |     |     |       |     |     |
|       |     |     | 293   | +17 | + 2 |       |     |     |       |     |     |

По крайней мере на первый взгляд мы не замечаем связи между значениями чисел  $a$ ,  $b$ , которым соответствует одна и та же совокупность. Однако, если мы учтем, что подобное различие в теории квадратичных вычетов относительно числа  $-3$  устанавливается по более простым правилам, чем относительно числа  $+3$ , то у нас появляется надежда на такое же счастливое обстоятельство и в теории биквадратичных вычетов. И действительно, мы находим, что число  $-3$  принадлежит

## совокупности:

| A для |      |      | B для |      |      | C для |      |      | D для |      |      |
|-------|------|------|-------|------|------|-------|------|------|-------|------|------|
| $p$   | $a$  | $b$  | $p$   | $a$  | $b$  | $p$   | $a$  | $b$  | $p$   | $a$  | $b$  |
| 37    | + 1  | — 6  | 5     | + 1  | + 2  | 13    | — 3  | + 2  | 29    | + 5  | + 2  |
| 61    | + 5  | — 6  | 17    | + 1  | — 4  | 73    | — 3  | — 8  | 41    | + 5  | — 4  |
| 157   | + 11 | — 6  | 89    | + 5  | — 8  | 97    | + 9  | + 4  | 53    | — 7  | + 2  |
| 193   | — 7  | — 12 | 113   | — 7  | — 8  | 109   | — 3  | + 10 | 101   | + 1  | + 10 |
|       |      |      | 137   | — 11 | — 4  | 181   | + 9  | + 10 | 197   | + 1  | — 14 |
|       |      |      | 149   | — 7  | + 10 | 229   | — 15 | + 2  | 269   | + 13 | + 10 |
|       |      |      | 173   | + 13 | + 2  | 241   | — 15 | — 4  | 293   | + 17 | + 2  |
|       |      |      | 233   | + 13 | + 8  | 277   | + 9  | + 14 |       |      |      |
|       |      |      | 257   | + 1  | — 16 |       |      |      |       |      |      |
|       |      |      | 281   | + 5  | + 16 |       |      |      |       |      |      |

и здесь индуктивный закон немедленно бросается в глаза.

Именно, число  $-3$  принадлежит совокупности

$A$ , если  $b$  делится на 3, т. е.  $b \equiv 0 \pmod{3}$ ,

$B$ , если  $a + b$  делится на 3, т. е.  $b \equiv 2a \pmod{3}$ ,

$C$ , если  $a$  делится на 3, т. е.  $a \equiv 0 \pmod{3}$ ,

$D$ , если  $a - b$  делится на 3. т. е.  $b \equiv a \pmod{3}$ .

## 26

Далее, мы находим, что число  $+5$  принадлежит совокупности

$A$  для  $p = 101, 109, 149, 181, 269$ ,

$B$  для  $p = 13, 17, 73, 97, 157, 193, 197, 233, 277, 293$ ,

$C$  для  $p = 29, 41, 61, 89, 229, 241, 281$ ,

$D$  для  $p = 37, 53, 113, 137, 173, 257$ .

Если мы рассмотрим значения чисел  $a, b$ , которые соответствуют отдельным  $p$ , то мы подметим здесь закон так же легко, как и при классификации числа  $-3$ . Именно, число  $+5$  оказывается в совокупности

$A$ , если  $b \equiv 0 \pmod{5}$ ,

$B$ , если  $b \equiv a$ ,

$C$ , если  $a \equiv 0$ ,

$D$ , если  $b \equiv 4a$ .



Очевидно, что эти правила охватывают все случаи, так как для  $b \equiv 2a$  или  $b \equiv 3a \pmod{5}$  имело бы место  $a^2 + b^2 \equiv 0$ , что невозможно, ибо, по предположению, простое число  $p$  отлично от 5.

## 27

Точно так же индуктивное рассмотрение, примененное к числам  $-7, -11, +13, +17, -19, -23$  и продолженное достаточно далеко, дает следующие правила.

Для числа  $-7$

|     |                                          |
|-----|------------------------------------------|
| $A$ | $a \equiv 0$ или $b \equiv 0 \pmod{7}$ , |
| $B$ | $b \equiv 4a$ или $b \equiv 5a$ ,        |
| $C$ | $b \equiv a$ или $b \equiv 6a$ ,         |
| $D$ | $b \equiv 2a$ или $b \equiv 3a$ .        |

Для числа  $-11$

|     |                                           |
|-----|-------------------------------------------|
| $A$ | $b \equiv 0, 5a$ или $6a \pmod{11}$ ,     |
| $B$ | $b \equiv a, 3a$ или $4a$ ,               |
| $C$ | $a \equiv 0$ или $b \equiv 2a$ или $9a$ , |
| $D$ | $b \equiv 7a, 8a$ или $10a$ .             |

Для числа  $+13$

|     |                                  |
|-----|----------------------------------|
| $A$ | $b \equiv 0, 4a, 9a \pmod{13}$ , |
| $B$ | $b \equiv 6a, 11a, 12a$ ,        |
| $C$ | $a \equiv 0; b \equiv 3a, 10a$ , |
| $D$ | $b \equiv a, 2a, 7a$ .           |

Для числа  $+17$

|     |                                              |
|-----|----------------------------------------------|
| $A$ | $a \equiv 0; b \equiv 0, a, 16a \pmod{17}$ , |
| $B$ | $b \equiv 2a, 6a, 8a, 14a$ ,                 |
| $C$ | $b \equiv 5a, 7a, 10a, 12a$ ,                |
| $D$ | $b \equiv 3a, 9a, 11a, 15a$ .                |

Для числа  $-19$ 

|     |                                           |
|-----|-------------------------------------------|
| $A$ | $b \equiv 0, 2a, 5a, 14a, 17a \pmod{19},$ |
| $B$ | $b \equiv 3a, 7a, 11a, 13a, 18a,$         |
| $C$ | $a \equiv 0; b \equiv 4a, 9a, 10a, 15a,$  |
| $D$ | $b \equiv a, 6a, 8a, 12a, 16a.$           |

Для числа  $-23$ 

|     |                                                        |
|-----|--------------------------------------------------------|
| $A$ | $a \equiv 0; b \equiv 0, 7a, 10a, 13a, 16a \pmod{23},$ |
| $B$ | $b \equiv 2a, 3a, 4a, 11a, 15a, 17a,$                  |
| $C$ | $b \equiv a, 5a, 9a, 14a, 18a, 22a,$                   |
| $D$ | $b \equiv 6a, 8a, 12a, 19a, 20a, 21a.$                 |

## 28

Найденные таким способом при индуктивном рассмотрении специальные теоремы оказываются верными, сколь далеко мы бы ни продолжали индукцию, и дают очень красивую форму критериев. Если же сравнить их между собой, чтобы сделать общие выводы, то с первого же взгляда приходят на мысль *следующие замечания*.

Критерии, при помощи которых узнается, к какому классу принадлежит простое число  $\pm q$  (где берется верхний или нижний знак в зависимости от того, имеет ли  $q$  вид  $4n + 1$  или  $4n + 3$ ), зависят от чисел  $a, b$ , если сравнивать их между собой в отношении модуля  $q$ .

I. Именно, если  $a \equiv 0 \pmod{q}$ , то  $\pm q$  принадлежит определенной совокупности, причем этой совокупностью является  $A$  для  $q = 7, 17, 23$ , и  $C$  для  $q = 3, 11, 13, 19$ , из чего можно предположить, что первый случай имеет место вообще тогда, когда  $q$  имеет вид  $8n \pm 1$ , а второй, — когда  $q$  имеет вид  $8n \pm 3$ . Совокупности же  $B$  и  $D$  уже заранее исключаются для делящегося на  $q$  значения  $a$ , так как в этом случае  $p \equiv b^2 \pmod{q}$ , т. е.  $p$  является квадратичным вычетом числа  $q$ , а потому, в силу фундаментальной теоремы,  $\pm q$  должно быть квадратичным вычетом числа  $p$ .

II. Если же  $a$  не делится на  $q$ , то критерий зависит от значения выражения  $\frac{b}{a} \pmod{q}$ . Это выражение может иметь, вообще

говоря, одно из  $q$  различных значений, а именно, значений  $0, 1, 2, 3, \dots, q-1$ ; но если  $q$  имеет вид  $4n+1$ , то исключаются оба значения выражения  $\sqrt{-1} \pmod{q}$ , которые заведомо не могут быть значениями выражения  $\frac{b}{a} \pmod{q}$ , потому что все время предполагается, что  $p = a^2 + b^2$  является простым числом, отличным от  $q$ . Поэтому число допустимых значений выражения  $\frac{b}{a} \pmod{q}$  для  $q \equiv 1 \pmod{4}$  равно  $q-2$ , в то время как для  $q \equiv 3 \pmod{4}$  оно остается равным  $q$ .

Теперь эти значения распадаются на четыре класса, именно, так, что одни, обозначаемые в общем виде через  $\alpha$ , соответствуют совокупности  $A$ , другие, обозначаемые через  $\beta$ , — совокупности  $B$ , третьи, обозначаемые через  $\gamma$ , — совокупности  $C$ , и четвертые, обозначаемые через  $\delta$ , — совокупности  $D$ , причем так, что  $\pm q$  принадлежит совокупности  $A, B, C, D$ , если соответственно имеет место  $b \equiv \alpha a, b \equiv \beta a, b \equiv \gamma a, b \equiv \delta a \pmod{q}$ .

Однако закон этого разбиения оказывается лежащим довольно глубоко, хотя некоторые общие замечания и могут быть сделаны сразу же. Число значений в трех классах одинаково, а именно, равно  $(q-1)/4$  или  $(q+1)/4$ , в то время как в четвертом классе (причем в том, который соответствует совокупности с критерием  $a \equiv 0$ ) оно на единицу меньше, так что число всех различных критериев относительно отдельных совокупностей одинаково, именно, равно  $(q-1)/4$  или  $(q+1)/4$ . Далее, заметим, что число 0 всегда встречается в первом классе (среди чисел,  $\alpha$ ), а дополнения чисел  $\alpha, \beta, \gamma, \delta$  до  $q$ , т. е. числа  $q-\alpha, q-\beta, q-\gamma, q-\delta$  содержатся соответственно в первом, четвертом, третьем, втором классах. Наконец, мы видим, что значения выражений  $\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}, \frac{1}{\delta} \pmod{q}$  принадлежат к первому, четвертому, третьему, второму классам, если критерий  $a \equiv 0$  соответствует совокупности  $A$ , и, напротив, третьему, второму, первому, четвертому классам, если критерий  $a \equiv 0$  относится к совокупности  $C$ . Этим ограничивается то, что может быть обнаружено индуктивным путем, если мы не хотим позволить себе предвидеть также и то, что ниже будет выведено из естественных источников.

Прежде чем идти дальше, мы хотим отметить, что *знание критериев для простых чисел* (взятых положительными, если они имеют вид  $4n + 1$ , и отрицательными, если они имеют вид  $4n + 3$ ) *достаточно для того, чтобы классифицировать все остальные числа*, если только использовать теорему из п. 7 и критерии для чисел  $-1$  и  $\pm 2$ . Так, например, если мы хотим иметь критерии для числа  $+3$ , то оказывается, что указанные в п. 25 критерии, касающиеся числа  $-3$ , имеют силу также и для  $+3$ , если число  $b/2$  четно, а если оно нечетно, то в этих критериях совокупности  $A, B, C, D$  заменяются соответственно на  $C, D, A, B$ , так что мы получаем следующие правила.

Число  $+3$  принадлежит

| совокупности | если                                                                                     |
|--------------|------------------------------------------------------------------------------------------|
| $A$          | $b \equiv 0 \pmod{12}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 2 \pmod{4}$ ;  |
| $B$          | $b \equiv 8a$ или $10a \pmod{12}$ ,                                                      |
| $C$          | $b \equiv 6a \pmod{12}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 0 \pmod{4}$ , |
| $D$          | $b \equiv 2a$ или $4a \pmod{12}$ .                                                       |

Точно так же критерии для  $\pm 6$  выводятся из критериев для  $\mp 2$  и  $-3$ .

Число  $+6$  принадлежит

| совокупности | если                                                                                                 |
|--------------|------------------------------------------------------------------------------------------------------|
| $A$          | $b \equiv 0, 2a, 22a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 4a \pmod{8}$ ,    |
| $B$          | $b \equiv 4a, 6a, 8a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 2a \pmod{8}$ ,    |
| $C$          | $b \equiv 10a, 12a, 14a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 0 \pmod{8}$ ,  |
| $D$          | $b \equiv 16a, 18a, 20a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$ и $b \equiv 6a \pmod{8}$ . |

Число же  $-6$  принадлежит

| совокупности | если                                                                                                   |
|--------------|--------------------------------------------------------------------------------------------------------|
| $A$          | $b \equiv 0, 10a, 14a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$<br>и $b \equiv 4a \pmod{8}$ .  |
| $B$          | $b \equiv 4a, 8a, 18a \pmod{24}$ или одновременно $a \equiv 0 \pmod{3}$<br>и $b \equiv 6a \pmod{8}$ ,  |
| $C$          | $b \equiv 2a, 12a, 22a \pmod{24}$ или одновременно<br>$a \equiv 0 \pmod{3}$ и $b \equiv 0 \pmod{8}$ ,  |
| $D$          | $b \equiv 6a, 16a, 20a \pmod{24}$ или одновременно<br>$a \equiv 0 \pmod{3}$ и $b \equiv 2a \pmod{8}$ . |

Аналогичным образом критерии для числа  $+21$  составляются из критериев для чисел  $-3$  и  $-7$ , критерии для числа  $-105$  — из критериев для чисел  $-1$ ,  $-3$ ,  $+5$ ,  $-7$  и т. д.

### 30

Итак, индукция приносит нам богатый урожай специальных теорем, которые родственны теореме о числе 2; однако между ними отсутствует общая связь, отсутствуют строгие доказательства, так как метод, которым мы в первом сочинении рассматривали число 2, дальше уже неприменим. Правда, нет недостатка в различных методах, при помощи которых можно получить доказательства для частных случаев, в первую очередь тех, которые относятся к распределению квадратичных вычетов по совокупностям  $A$  и  $C$ ; однако мы не будем на них останавливаться, ибо мы должны желать построить общую теорию, охватывающую все случаи. После того как мы еще в 1805 г. начали размышлять об этом предмете, мы скоро пришли к убеждению, что *естественный источник общей теории следует искать в расширении области арифметики*, как мы уже указывали в п. 1.

Именно, в то время как в рассматривавшихся до сих пор вопросах высшая арифметика имеет дело только с целыми вещественными числами, теоремы, относящиеся к биквадратичным вычетам, только тогда выступают во всей своей простоте и естественной красоте, когда

область арифметики распространяется также и на мнимые числа, так что ее объектом становятся без ограничения все числа вида  $a + bi$ , где, как обычно,  $i$  обозначает мнимую величину  $\sqrt{-1}$ , а  $a$  и  $b$  — всевозможные целые вещественные числа от  $-\infty$  до  $+\infty$ . Такие числа мы будем называть целыми комплексными числами, причем вещественные числа не противопоставляются комплексным, а рассматриваются как их частный случай. Настоящее сочинение будет содержать как элементарное учение о комплексных величинах, так и начала теории биквадратичных вычетов, полное развитие которой мы поставим себе целью в продолжении этой работы \*.

## 31

Прежде всего мы предпошлем некоторые наименования, введение которых будет способствовать большей краткости и ясности.

Область комплексных чисел  $a + bi$  содержит:

I. Вещественные числа, у которых  $b = 0$ , и среди них, в зависимости от того, каково число  $a$ ,

- 1) нуль,
- 2) положительные числа,
- 3) отрицательные числа.

II. Мнимые числа, у которых  $b$  отлично от нуля. Здесь снова различаются:

- 1) мнимые числа без вещественной части, т. е. такие, у которых  $a = 0$ ,
- 2) мнимые числа с вещественной частью, т. е. такие, у которых ни  $a$ , ни  $b$  не равны нулю.

Первые, при желании, можно называть чисто мнимыми числами, а вторые — смешанными мнимыми числами.

---

\* Мы хотим только заметить еще, что подобное расширение области теории биквадратичных вычетов особенно целесообразно. Теория кубических вычетов подобным же образом должна основываться на рассмотрении чисел вида  $a + bh$ , где  $h$  есть некоторый мнимый корень уравнения  $h^3 - 1 = 0$ , например,  $h = -\frac{1}{2} + \sqrt{\frac{3}{4}} i$ , и точно так же теория вычетов более высоких степеней требует введения других мнимых величин.

В настоящей теории мы будем употреблять четыре единицы:  $+1$ ,  $-1$ ,  $+i$ ,  $-i$ , которые кратко будут называться соответственно положительной, отрицательной, положительно мнимой и отрицательно мнимой единицами.

Три произведения некоторого комплексного числа на одно из чисел  $-1$ ,  $+i$ ,  $-i$  мы будем называть числами, ассоциированными с этим числом. За исключением нуля (который ассоциирован с самим собой), всегда, таким образом, ассоциированы одно с другим четыре различных числа.

Напротив, число, которое получается из данного комплексного числа заменой  $i$  на  $-i$ , мы будем называть сопряженным с этим числом. Таким образом, мнимые числа разбиваются на пары различных между собой сопряженных чисел, в то время как вещественные числа сопряжены сами с собой, если только мы хотим использовать этот термин и для них.

Произведение комплексного числа на число, сопряженное с ним, мы назовем нормой каждого из этих чисел. Для вещественного числа в качестве нормы должен рассматриваться, следовательно, его квадрат.

Вообще мы имеем по восемь связанных между собой чисел, именно:

$$\begin{array}{c|c} a + bi & a - bi \\ -b + ai & -b - ai \\ -a - bi & -a + bi \\ b - ai & b + ai; \end{array}$$

здесь мы видим две четверки ассоциированных чисел и четыре пары сопряженных чисел, а общая норма их всех равна  $a^2 + b^2$ . Однако среди этих восьми чисел будет только четыре различных, если либо  $a = \pm b$ , либо одно из чисел  $a$ ,  $b$  равно 0.

Из приведенных определений тотчас же получается такое следствие.

Числом, сопряженным с произведением двух комплексных чисел, является произведение чисел, сопряженных с ними.

Так же обстоит дело и для произведения большего числа сомножителей и для частного.

*Норма произведения двух комплексных чисел равна произведению норм этих чисел.*

Эта теорема также распространяется на произведение любого числа сомножителей и на отношения.

*Норма каждого комплексного числа (за исключением нуля, что мы, начиная отсюда, будем в большинстве случаев молчаливо предполагать) является положительным числом.*

Далее, ничто не мешает распространить наши определения на дробные или иррациональные значения чисел  $a, b$ ; однако  $a + bi$  только тогда будет называться целым комплексным числом, когда каждое из чисел  $a, b$  целое, и только тогда рациональным, когда каждое из чисел  $a, b$  рационально.

### 32

Алгоритм арифметических операций над комплексными числами хорошо известен; деление посредством введения нормы может быть сведено к умножению, так как мы имеем

$$\frac{a + bi}{c + di} = (a + bi) \frac{c - di}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i.$$

Квадратный корень извлекается по формуле

$$\sqrt{a + bi} = \pm \left( \sqrt{\frac{V_{a^2 + b^2} + a}{2}} + i \sqrt{\frac{V_{a^2 + b^2} - a}{2}} \right),$$

если  $b$  является положительным числом, или по формуле

$$\sqrt{a + bi} = \pm \left( \sqrt{\frac{V_{a^2 + b^2} + a}{2}} - i \sqrt{\frac{V_{a^2 + b^2} - a}{2}} \right),$$

если  $b$  является отрицательным числом. На том, какую пользу в смысле облегчения операций играет преобразование комплексных чисел  $a + bi$  к виду  $r(\cos \varphi + i \sin \varphi)$ , нам нет здесь нужды останавливаться.



Целое комплексное число, которое может быть разложено на два отличных от единиц сомножителя\*, мы будем называть **составным комплексным числом**; напротив, число, не допускающее такого разложения, называется **комплексным простым числом**. Из этого тотчас же вытекает, что каждое составное вещественное число является также и составным комплексным числом. *Однако вещественное простое число может быть составным комплексным числом, а именно, это будет иметь место для числа 2 и всех вещественных положительных простых чисел вида  $4n + 1$  (за исключением числа 1), так как они, как известно, могут быть разложены на два положительных квадрата; например,  $2 = (1 + i)(1 - i)$ ,  $5 = (1 + 2i)(1 - 2i)$ ,  $13 = (3 + 2i)(3 - 2i)$ ,  $17 = (1 + 4i)(1 - 4i)$  и т. д.*

*Напротив, положительные вещественные простые числа вида  $4n + 3$  всегда являются также и комплексными простыми числами.* Действительно, если бы для некоторого такого числа имело место  $q = (a + bi)(\alpha + \beta i)$ , то было бы также  $q = (a - bi)(\alpha - \beta i)$ , и потому  $q^2 = (a^2 + b^2)(\alpha^2 + \beta^2)$ ; но  $q$  может быть только одним единственным способом разложено на положительные сомножители, большие чем 1, именно,  $q^2 = q \cdot q$ , так что должно было бы быть  $q = a^2 + b^2 = \alpha^2 + \beta^2$ . Это, однако, невозможно, так как сумма двух квадратов не может иметь вид  $4n + 3$ .

Для отрицательных вещественных чисел, очевидно, сохраняет силу та же терминология, что и для положительных, и так же обстоит дело и для чисто мнимых чисел.

*Остается поэтому только показать, как отличать составные числа от простых среди смешанных мнимых чисел, и это достигается следующей теоремой.*

**Теорема.** *Каждое целое смешанное мнимое число  $a + bi$  является или комплексным простым числом, или составным числом, в зависимости от того, является ли его норма простым вещественным числом или составным числом.*

---

\* Или, что то же самое, на такие сомножители, нормы которых больше единицы.

**Доказательство.** I. Так как норма составного комплексного числа всегда является составным числом, то очевидно, что комплексное число, норма которого является вещественным простым числом, обязательно должно быть комплексным простым числом. Это первая часть теоремы.

II. Если же норма  $a^2 + b^2$  является составным числом, то пусть  $p$  — вещественное положительное простое число, которое входит в нее делителем. Рассмотрим тогда два случая.

1. Если  $p$  имеет вид  $4n + 3$ , то, как известно,  $a^2 + b^2$  может делиться на  $p$  только тогда, когда  $p$  одновременно входит и в  $a$  и в  $b$ , так что  $a + bi$  будет составным числом.

2. Если  $p$  не имеет вида  $4n + 3$ , то оно заведомо может быть разложено на два квадрата; положим поэтому  $p = \alpha^2 + \beta^2$ .

Так как

$$(a\alpha + b\beta)(a\alpha - b\beta) = a^2(\alpha^2 + \beta^2) - \beta^2(a^2 + b^2),$$

и потому левая часть делится на  $p$ , то  $p$  заведомо будет входить в один из сомножителей  $a\alpha + b\beta$ ,  $a\alpha - b\beta$ , а так как, далее,

$$(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 = (a\alpha - b\beta)^2 + (b\alpha + a\beta)^2 = (a^2 + b^2)(\alpha^2 + \beta^2),$$

и потому левая часть делится на  $p^2$ , то очевидно, что в первом случае на  $p$  должно делиться также число  $b\alpha - a\beta$ , а во втором — число  $b\alpha + a\beta$ . Поэтому в первом случае будет целым комплексным числом

$$\frac{a + bi}{\alpha + \beta i} = \frac{a\alpha + b\beta}{p} + \frac{b\alpha - a\beta}{p} i,$$

а во втором — число

$$\frac{a + bi}{\alpha - \beta i} = \frac{a\alpha - b\beta}{p} + \frac{b\alpha + a\beta}{p} i.$$

Так как вследствие этого заданное число делится или на  $\alpha + \beta i$ , или на  $\alpha - \beta i$ , и норма отношения, именно,  $(a^2 + b^2)/p$ , по предположению, отлична от единицы, то  $a + bi$  в обоих случаях является комплексным составным числом. Это вторая часть теоремы.

## 34

Таким образом, совокупность комплексных простых чисел исчерпывается числами следующих четырех типов.

1. Четырьмя единицами  $1, +i, -1, -i$ , которые, однако, когда речь будет идти о простых числах, мы в большинстве случаев молчаливо будем предполагать исключенными.

2. Числом  $1 + i$  и тремя ассоциированными с ним числами  $-1 + i, -1 - i, 1 - i$ .

3. Вещественными положительными простыми числами вида  $4n + 3$  и тройками чисел, ассоциированных с каждым из них.

4. Комплексными числами, нормами которых являются превосходящие единицу простые числа вида  $4n + 1$ , причем каждой данной норме такого вида соответствует в точности по восемь комплексных простых чисел, так как такая норма только одним единственным образом может быть разложена на два квадрата.

## 35

Точно так же, как вещественные целые числа разделяются на четные и нечетные, а первые снова на делящиеся на 4 и не делящиеся на 4, так и для комплексных чисел имеет место столь же важное различие. Именно, комплексные числа или не делятся на  $1 + i$ , например, числа  $a + bi$ , у которых одно из чисел  $a, b$  нечетно, а другое четно, или делятся на  $1 + i$ , но не делятся на 2, если каждое из чисел  $a, b$  нечетно, или делятся на 2, если каждое из чисел  $a, b$  четно.

Числа первого класса удобно называть нечетными, числа второго класса — получетными, а числа третьего класса — четными комплексными числами.

Произведение нескольких комплексных сомножителей всегда нечетно, если все сомножители нечетны; оно получетно, если один из сомножителей получетен, а остальные нечетны; наконец, оно четно, если среди сомножителей имеются или по крайней мере два получетных, или по крайней мере один четный.

Норма каждого нечетного комплексного числа имеет вид  $4n + 1$ ; норма получетного числа имеет вид  $8n + 2$ ; наконец, норма четного числа является произведением числа вида  $4n + 1$  на число 4 или на большую степень числа 2.

Так как связь между четырьмя ассоциированными комплексными числами аналогична связи между двумя противоположными вещественными числами (т. е. между двумя числами, равными по абсолютной величине, но имеющими противоположные знаки), а из них положительное обычно по праву рассматривается как первичное, то возникает вопрос, может ли быть подобным же образом выделено одно число из каждых четырех ассоциированных комплексных чисел и будет ли это полезным? Чтобы решить этот вопрос, нужно учесть, что принцип выделения должен быть таким, что произведение двух чисел, которые среди ассоциированных с ними рассматриваются как первичные, всегда должно быть первичным числом среди чисел, ассоциированных с ним. Но мы сейчас же убеждаемся, что такого принципа вообще не существует, если выделение первичного числа не ограничивать только целыми числами; полезным же такое выделение оказывается лишь для нечетных чисел. А для них поставленная цель может быть достигнута следующими двумя способами.

I. Произведение двух чисел  $a + bi$ ,  $a' + b'i$  с тем свойством, что  $a$  и  $a'$  имеют вид  $4n + 1$ , а  $b$  и  $b'$  четны, снова обладает этим свойством, т. е. его вещественная часть будет  $\equiv 1 \pmod{4}$ , а мнимая часть будет четной. Но легко видеть, что среди четырех ассоциированных нечетных чисел всегда будет одно и только одно число с таким свойством.

II. Если число  $a + bi$  обладает тем свойством, что  $a \equiv 1$  и  $b$  или одновременно делятся на 4 или одновременно делятся на 2, но не делятся на 4, то произведение его на комплексное число такого же вида будет обладать этим же свойством, и легко видеть, что из каждых четырех ассоциированных нечетных чисел числом такого вида будет одно и только одно.

Из этих двух приблизительно одинаково целесообразных принципов мы выберем второй; именно, среди четырех ассоциированных нечетных комплексных чисел мы будем рассматривать как первичное то число, которое по модулю  $2 + 2i$  сравнимо с положительной единицей; благодаря этому мы сможем намного короче формулировать многие замечательные теоремы. Так, например, первичными

являются комплексные простые числа  $-1+2i$ ,  $-1-2i$ ,  $+3+2i$ ,  $+3-2i$ ,  $+1+4i$ ,  $+1-4i$ , ..., так же, как и вещественные отрицательные простые числа  $-3$ ,  $-7$ ,  $-11$ ,  $-19$ , ... Число, сопряженное с нечетным комплексным первичным числом, тоже будет первичным.

Для получетных и четных чисел вообще такое различие было бы слишком произвольным и почти бесполезным. Хотя среди ассоциированных простых чисел  $1+i$ ,  $1-i$ ,  $-1+i$ ,  $-1-i$  мы и можем выбрать одно число в качестве первичного, но для составных чисел мы такого различия производить не будем.

### 37

Если среди сомножителей составного комплексного числа имеются такие, которые сами являются составными, и если они снова разложены на сомножители, то ясно, что в конце концов мы придем к простым сомножителям, т. е. *каждое составное число разложимо на простые сомножители*. Если среди них имеются не первичные сомножители, то мы подставим вместо них произведения ассоциированных с ними первичных чисел на  $i$ ,  $-1$  или  $-i$ . Таким образом, мы получаем, что каждое составное комплексное число  $M$  может быть представлено в виде

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \dots,$$

где  $A$ ,  $B$ ,  $C$ , ... являются различными между собой простыми комплексными первичными числами, и  $\mu = 0, 1, 2$  или  $3$ . Для такого разложения справедлива теорема, что оно возможно лишь одним единственным образом, — теорема, которая при поверхностном рассмотрении могла бы показаться очевидной сама собой, однако, в действительности требующая доказательства. К нему пролагает путь следующая теорема.

**Теорема.** *Произведение  $M = A^{\alpha} B^{\beta} C^{\gamma} \dots$ , где  $A$ ,  $B$ ,  $C$ , ... обозначают различные простые комплексные первичные числа, не может делиться ни на одно первичное комплексное простое число, не содержащееся среди чисел  $A$ ,  $B$ ,  $C$ , ...*

**Доказательство.** Пусть  $P$  — первичное комплексное простое число, не содержащееся среди чисел  $A$ ,  $B$ ,  $C$ , ..., и пусть  $p$ ,  $a$ ,  $b$ ,  $c$ , ...

являются соответственно нормами чисел  $P, A, B, C, \dots$ . Тогда легко видеть, что норма числа  $M$  равна  $a^\alpha b^\beta c^\gamma \dots$  так что это число должно было бы делиться на  $p$ , если бы  $M$  делилось на  $P$ . Так как отдельные нормы являются или вещественными простыми числами (из ряда  $2, 5, 13, 17, \dots$ ), или квадратами вещественных простых чисел (из ряда  $9, 49, 121, \dots$ ), то немедленно ясно, что это может быть только тогда, когда  $p$  равно одной из норм  $a, b, c, \dots$ ; мы предположим поэтому, что  $p = a$ . Но так как, по предположению,  $P$  и  $A$  являются различными между собой первичными комплексными простыми числами, то легко видеть, что это может выполняться лишь если  $P$  и  $A$  являются сопряженными комплексными числами, и потому  $p = a$  является нечетным вещественным простым числом (а не квадратом простого числа); положим поэтому  $A = k + li, P = k - li$ . Тогда (если распространить понятие и обозначение для сравнимости на целые комплексные числа) будет иметь место  $A \equiv 2k \pmod{P}$ , откуда легко видеть, что

$$M \equiv 2^\alpha k^\alpha B^\beta C^\gamma \dots \pmod{P}.$$

Таким образом, если предположить, что  $M$  делится на  $P$ , то и

$$2^\alpha k^\alpha B^\beta C^\gamma \dots$$

будет делиться на  $P$ , а потому норма этого числа, которая равна

$$2^{2\alpha} k^{2\alpha} b^\beta c^\gamma \dots,$$

будет делиться на  $p$ . Но так как  $2$  и  $k$  заведомо на  $p$  не делятся, то из этого следует, что  $p$  должно совпадать с одним из чисел  $b, c, \dots$ . Пусть, например,  $p = b$ . Но тогда мы заключаем отсюда, что или  $B = k + li$ , или  $B = k - li$ , т. е. или  $B = A$ , или  $B = P$ , но и то и другое противоречит предположению.

Из этой теоремы другая теорема, а именно, что разложение на простые сомножители возможно только единственным способом, выводится очень легко, причем методом, совершенно аналогичным тому, который мы использовали в «Арифметических исследованиях» (п. 16); поэтому было бы излишним задерживаться сейчас на этом.

Теперь мы переходим к *сравнимости чисел по комплексным модулям*. Однако до начала этого исследования целесообразно показать, как комплексные числа можно наглядно интерпретировать.

Подобно тому, как каждая вещественная величина выражается куском бесконечной в обе стороны прямой линии, начинающимся из произвольно выбранной начальной точки и измеренным произвольно выбранным в качестве единицы отрезком, и потому может быть представлена другим концом этого куска, причем точки по одну сторону от начальной представляют положительные величины, а точки по другую сторону от начальной — отрицательные, так и каждая комплексная величина может быть представлена некоторой точкой бесконечной плоскости, на которой определенная прямая служит для представления вещественных величин; а именно, комплексная величина  $x + iy$  представляется точкой, абсцисса которой равна  $x$ , а ордината (берущаяся положительной по одну сторону от линии абсцисс и отрицательной — по другую сторону) равна  $y$ . Таким образом, можно говорить, что каждая комплексная величина измеряет различие между положением той точки, которой представляется эта величина, и положением начала координат, если положительная единица обозначает произвольное, но фиксированное отклонение по произвольному, но фиксированному направлению, отрицательная единица — такое же по величине отклонение по противоположному направлению, наконец, мнимые единицы — такие же по величине отклонения по направлениям, перпендикулярным первым, и идущим в обе стороны.

Таким образом, на природу величин, которые мы называем мнимыми, проливается ясный свет. Если начало координат обозначить через  $(0)$ , а две комплексные величины  $m$ ,  $m'$  соответствуют точкам  $M$ ,  $M'$ , положение которых по отношению к точке  $(0)$  они выражают, то разность  $m - m'$  будет выражать не что иное, как положение точки  $M$  относительно точки  $M'$ ; с другой стороны, если произведение  $mm'$  выражает положение точки  $N$  относительно точки  $(0)$ , то легко убедиться, что это положение так же определяется положением точки  $M$  относительно точки  $(0)$ , как положение точки  $M'$  определяется положением той точки, которой

соответствует положительная единица, так что будет не лишено оснований сказать, что положения точек, соответствующих комплексным величинам  $mm'$ ,  $m$ ,  $m'$ ,  $1$ , образуют пропорцию. Однако более исчерпывающее изложение этого вопроса мы оставим до другого случая. Трудности, которыми считается окруженной теория мнимых величин, по большей части имеют своей причиной мало удачные наименования (некоторые снабдили их даже неудачно звучащим названием невозможных величин). Если бы, исходя из представлений, даваемых многообразием двух измерений (которые с большой ясностью проявляются при пространственных соображениях), называть положительные величины прямыми, отрицательные — обратными, а мнимые — к ним перпендикулярными величинами, то мы имели бы простоту вместо путаницы, ясность вместо туманности.

## 39

Изложенное в предыдущем пункте относится к непрерывным комплексным величинам; в арифметике же, которая имеет дело только с целыми числами, схемой комплексных чисел является система точек, так расположенных на одинаковых расстояниях одна от другой на проходящих на одинаковых расстояниях одна от другой прямых, что они разбивают бесконечную плоскость на бесконечное число квадратов. Все числа, делящиеся на заданное комплексное число  $a + bi = m$ , также будут образовывать бесконечно много квадратов, стороны которых равны  $\sqrt{a^2 + b^2}$ , т. е. площади равны  $a^2 + b^2$ ; если ни одно из чисел  $a$ ,  $b$  не равно нулю, то последние квадраты будут расположены по отношению к первым наклонно. Каждому числу, не делящемуся на модуль  $m$ , будет соответствовать точка, расположенная или внутри одного из таких квадратов, или на границе двух квадратов; последний случай, однако, может иметь место только тогда, когда числа  $a$ ,  $b$  имеют общий делитель; далее, ясно, что числа, сравнимые по модулю  $m$ , занимают в своих квадратах конгруэнтные положения. Отсюда легко видеть, что если собрать все числа, лежащие внутри некоторого определенного квадрата, и все числа, лежащие на каких-нибудь двух не противоположных его сторонах, и, наконец, добавить к ним число, делящееся на  $m$ , то мы получим полную систему несравнимых по модулю  $m$  вычетов,



т. е. каждое целое число будет сравнимо с одним и только одним из этих чисел. Было бы также нетрудно показать, что количество этих вычетов равно норме модуля, т. е. равно  $a^2 + b^2$ . Однако нам кажется целесообразным доказать эту очень важную теорему другим, чисто арифметическим, способом.

## 40

**Теорема.** По заданному комплексному модулю  $m = a + bi$ , норма которого равна  $a^2 + b^2 = p$  и для которого  $a, b$  являются взаимно простыми числами, каждое целое комплексное число сравнимо с одним и только одним вычетом из ряда  $0, 1, 2, 3, \dots, p - 1$ .

**Доказательство.** I. Если  $\alpha, \beta$  являются целыми числами, для которых имеет место  $\alpha a + \beta b = 1$ , то

$$i = \alpha b - \beta a + m(\beta + \alpha i).$$

Если поэтому дано целое комплексное число  $A + Bi$ , то

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha Bi).$$

Поэтому, если обозначить через  $h$  наименьший положительный вычет числа  $A + (\alpha b - \beta a)B$  по модулю  $p$  и положить

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki),$$

то будет выполняться равенство

$$A + Bi = h + m[\beta B + ak + (\alpha B - bk)i],$$

или

$$A + Bi \equiv h \pmod{m}.$$

Тем самым доказана первая часть теоремы.

II. Если с некоторым комплексным числом сравнимы по модулю  $m$  два вещественных числа  $h, h'$ , то они будут сравнимы и между собой. Поэтому, если мы положим  $h - h' = m(c + di)$ , то будет выполняться равенство

$$(h - h')(a - bi) = p(c + di),$$

и потому

$$(h - h')a = pc, \quad (h - h')b = -pd,$$

и, далее, вследствие того, что  $a\alpha + b\beta = 1$ ,

$$h - h' = p(c\alpha - d\beta), \text{ т. е. } h \equiv h' \pmod{p}.$$

Поэтому числа  $h, h'$ , если они не равны, не могут оба одновременно содержаться в совокупности чисел  $0, 1, 2, 3, \dots, p-1$ . Тем самым доказана вторая часть теоремы.

## 41

**Теорема.** По комплексному модулю  $m = a + bi$ , норма которого равна  $a^2 + b^2 = p$  и для которого  $a, b$  не взаимно просты, а имеют наибольший общий делитель  $\lambda$  (который мы предполагаем положительным), каждое комплексное число сравнимо с вычетом  $x + iy$ , обладающим тем свойством, что  $x$  является одним из чисел  $0, 1, 2, 3, \dots, \frac{p}{\lambda} - 1$ , а  $y$  — одним из чисел  $0, 1, 2, 3, \dots, \lambda - 1$ , причем только с одним единственным из всех  $p$  вычетов, имеющих такой вид.

**Доказательство.** I. Если выбрать целые числа  $\alpha, \beta$  так, что  $\alpha a + \beta b = \lambda$ , то

$$\lambda i = \alpha b - \beta a + m(\beta + \alpha i).$$

Если теперь  $A + Bi$  — заданное комплексное число, далее, если  $y$  — наименьший положительный вычет числа  $B$  по модулю  $\lambda$ , и  $x$  — наименьший положительный вычет числа  $A + (\alpha b - \beta a) \frac{B-y}{\lambda}$  по модулю  $p/\lambda$ , и если положить

$$A + (\alpha b - \beta a) \frac{B-y}{\lambda} = x + \frac{p}{\lambda} \cdot k,$$

то будет иметь место

$$\begin{aligned} A + Bi - (x + yi) &= \frac{p}{\lambda} \cdot k + (B - y)i - (\alpha b - \beta a) \frac{B-y}{\lambda} = \\ &= \frac{p}{\lambda} \cdot k + \frac{B-y}{\lambda} \cdot m(\beta + \alpha i) = \left( \frac{a}{\lambda} - \frac{b}{\lambda} i \right) km + \frac{B-y}{\lambda} (\beta + \alpha i) m, \end{aligned}$$

т. е. стоящее слева число делится на  $m$ , а потому  $A + Bi \equiv x + yi \pmod{m}$ . Тем самым доказана первая часть теоремы.

II. Если мы предположим, что с одним и тем же комплексным числом сравнимы по модулю  $m$  два числа  $x + yi$  и  $x' + y'i$ , то они будут сравнимы по модулю  $m$  и между собой. Поэтому они тем более будут сравнимы по модулю  $\lambda$ , и потому  $y \equiv y' \pmod{\lambda}$ . Если теперь предположить, что каждое из чисел  $y, y'$  содержится среди

чисел  $0, 1, 2, 3, \dots, \lambda - 1$ , то обязательно должно быть  $y = y'$ . Но тогда будет иметь место также и  $x \equiv x' \pmod{m}$ , т. е.  $x - x'$  будет делиться на  $m$ , и потому число  $(x - x')/\lambda$  будет целым, делящимся на  $\frac{a}{\lambda} + \frac{b}{\lambda} i$ , т. е. будет выполняться сравнение

$$\frac{x - x'}{\lambda} \equiv 0 \pmod{\frac{a}{\lambda} + \frac{b}{\lambda} i}.$$

Но так как числа  $a/\lambda, b/\lambda$  взаимно просты, отсюда на основании второй части предыдущей теоремы следует, что  $(x - x')/\lambda$  делится также на норму числа  $\frac{a}{\lambda} + \frac{b}{\lambda} i$ , т. е. на число  $p/\lambda^2$ , а потому  $x - x'$  делится на  $p/\lambda$ . Поэтому, если предположить, что и каждое из чисел  $x, x'$  содержится в совокупности  $0, 1, 2, 3, \dots, \frac{p}{\lambda} - 1$ , то обязательно будет  $x = x'$ , т. е. вычеты  $x + yi, x' + y'i$  будут совпадать. Тем самым доказана вторая часть теоремы.

Между прочим, ясно, что сюда нужно причислять также случай, когда модуль является вещественным числом, т. е.  $b = 0$ , и потому  $\lambda = \pm a$ , и случай, когда модуль является чисто мнимым числом, т. е.  $a = 0$ , и потому  $\lambda = \pm b$ . В обоих случаях  $\frac{p}{\lambda} = \lambda$ .

## 42

Таким образом, если все сравнимые между собой по заданному модулю комплексные числа причислять к одному и тому же классу, а несравнимые — к различным классам, то всего будет  $p$  классов, охватывающих совокупность всех целых чисел, где  $p$  обозначает норму модуля. Совокупность такого же количества чисел, взятых из различных классов, будет давать полную систему несравнимых вычетов, которую мы научились выбирать в пп. 40 и 41. При этом выбор представителей в отдельных классах там основывался на том, что в каждом классе выбирался такой вычет  $x + yi$ , для которого  $y$  имеет наименьшее значение, а из нескольких вычетов с одинаковым наименьшим значением  $y$  — тот вычет, у которого значение  $x$  меньше всего, за исключением, однако, отрицательных значений как для  $x$ , так и для  $y$ . Но для других целей будет целесообразно придерживаться других принципов, причем особенно следует обра-

тить внимание на тот способ, при котором выбираются те вычеты, которые, будучи поделенными на модуль, дают самые простые частные. Очевидно, что если  $\alpha + \beta i$ ,  $\alpha' + \beta' i$ ,  $\alpha'' + \beta'' i, \dots$  являются частными, получающимися при делении на модуль сравнимых между собой чисел, то как разности между различными величинами  $\alpha, \alpha', \alpha'', \dots$ , так и разности между различными величинами  $\beta, \beta', \beta'', \dots$  будут целыми числами, и ясно, что всегда существует вычет, для которого  $\alpha$  и  $\beta$  лежат между границами 0 и 1, включая первую границу и исключая вторую; такой вычет мы будем называть просто **наименьшим вычетом**. При желании вместо указанных границ можно брать также границы  $-\frac{1}{2}$  и  $+\frac{1}{2}$  (включая первую и исключая вторую); вычеты, соответствующие этому ограничению, мы будем называть **абсолютно наименьшими вычетами**.

В отношении этих наименьших вычетов встают следующие задачи.

## 43

*Наименьший вычет заданного комплексного числа  $A + Bi$  по модулю  $a + bi$ , норма которого равна  $p$ , находят следующим образом.*

Если  $x + yi$  является искомым наименьшим вычетом, то  $(x + yi) \times (a - bi)$  будет наименьшим вычетом произведения  $(A + Bi)(a - bi)$  по модулю  $(a + bi)(a - bi)$ , т. е. по модулю  $p$ . Поэтому если положить

$$aA + bB = Fp + f, \quad aB - bA = Gp + g,$$

где  $f, g$  являются наименьшими вычетами чисел  $aA + bB$ ,  $aB - bA$  по модулю  $p$ , то выполняется равенство

$$x + yi = \frac{f + gi}{a - bi},$$

или

$$x = \frac{af - bg}{p} = A - aF + bG, \quad y = \frac{ag + bf}{p} = B - aG - bF.$$

Очевидно, что наименьшие вычеты  $f, g$  следует брать или в границах 0 и  $p - 1$ , или в границах  $-\frac{1}{2}p$  и  $+\frac{1}{2}p$  в зависимости от того, отыскивается ли просто наименьший или абсолютно наименьший вычет комплексного числа.

Нахождение полной системы наименьших вычетов для заданного модуля может быть выполнено несколькими способами. Первый метод состоит в том, что сначала определяются границы, между которыми должны лежать вещественные части, а затем для отдельных значений, лежащих между этими границами, находятся границы мнимых частей. Общий критерий наименьшего вычета  $x + yi$  для модуля  $a + bi$  состоит в том, что как  $ax + by = \xi$ , так и  $ay - bx = \eta$  лежат между границами 0 и  $a^2 + b^2$ , если речь идет просто о наименьших вычетах, или между границами  $-\frac{1}{2}(a^2 + b^2)$  и  $+\frac{1}{2}(a^2 + b^2)$ , если отыскиваются абсолютно наименьшие вычеты, причем вторая граница исключается. Специальные правила потребовали бы отдельного рассмотрения случаев, соответствующих различным возможностям для знаков чисел  $a$ ,  $b$ , но мы не будем тратить здесь время на их изложение, которое не связано ни с какими трудностями. Достаточно будет пояснить сущность метода на одном примере.

Для модуля  $5 + 2i$  просто наименьшие вычеты  $x + yi$  должны быть таковы, что как число  $5x + 2y = \xi$ , так и число  $5y - 2x = \eta$  равны одному из чисел  $0, 1, 2, 3, \dots, 28$ . Равенство  $29x = 5\xi - 2\eta$  показывает, что положительные значения  $x$  не могут быть больше чем  $5 \cdot 28 / 29$ , а абсолютные величины отрицательных значений не могут быть больше чем  $2 \cdot 28 / 29$ . Поэтому всевозможными допустимыми значениями для  $x$  являются следующие:  $-1, 0, 1, 2, 3, 4$ . Для  $x = -1$  число  $2y$  должно быть равно одному из значений  $5, 6, 7, \dots, 33$ , а число  $5y$  — одному из значений  $-2, -1, 0, 1, 2, 3, \dots, 26$ ; поэтому наименьшее значение для  $y$  равно  $+3$ , а наибольшее равно  $+5$ . Если так же рассмотреть остальные значения  $x$ , то получается следующая таблица всех наименьших вычетов:

| $x$  | $y$              |
|------|------------------|
| $-1$ | 3, 4, 5          |
| 0    | 0, 1, 2, 3, 4, 5 |
| $+1$ | 1, 2, 3, 4, 5, 6 |
| $+2$ | 1, 2, 3, 4, 5, 6 |
| $+3$ | 2, 3, 4, 5, 6    |
| $+4$ | 2, 3, 4          |

Подобным же образом для абсолютно наименьших вычетов значения  $\xi$  и  $\eta$  должны быть среди чисел  $-14, -13, -12, \dots, +14$ ; следовательно,  $29x$  не может лежать вне границ  $-7 \cdot 14$  и  $+7 \cdot 14$ , и потому  $x$  должен быть равен одному из чисел  $-3, -2, -1, 0, 1, 2, 3$ . Для  $x = -3$  число  $2y = \xi - 5x = \xi + 15$  будет равно одному из чисел  $1, 2, 3, \dots, 29$ , а число  $5y = \eta + 2x = \eta - 6$  — одному из чисел  $-20, -19, -18, \dots, +8$ . Отсюда для  $y$  получается единственное значение  $+1$ . Если таким же образом рассмотреть остальные значения  $x$ , то получается следующая таблица всех абсолютно наименьших вычетов:

| $x$  | $y$                     |
|------|-------------------------|
| $-3$ | $+1$                    |
| $-2$ | $-2, -1, 0, +1, +2$     |
| $-1$ | $-3, -2, -1, 0, +1, +2$ |
| $0$  | $-2, -1, 0, +1, +2$     |
| $+1$ | $-2, -1, 0, +1, +2, +3$ |
| $+2$ | $-2, -1, 0, +1, +2$     |
| $+3$ | $-1$                    |

## 45

При применении второго метода целесообразно различать два случая.

В первом случае, когда  $a$  и  $b$  не имеют общих делителей, положим  $\alpha a + \beta b = 1$ , и пусть  $k$  является наименьшим положительным вычетом числа  $\beta a - \alpha b$  по модулю  $p$ . Тогда тождественные соотношения

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b), \quad b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b)$$

показывают, что  $ak \equiv -b$ ,  $bk \equiv a \pmod{p}$ . Поэтому, если, как и выше, положить  $ax + by = \xi$ ,  $ay - bx = \eta$ , то будет иметь место  $\eta \equiv k\xi$ ,  $\xi \equiv -k\eta \pmod{p}$ . Таким образом, мы получим все числа  $\xi + \eta i$ , которые соответствуют просто наименьшим вычетам  $x + yi$ , если либо будем брать для  $\xi$  последовательно значения  $0, 1, 2, 3, \dots, p-1$ , а для  $\eta$  — наименьшие положительные вычеты произведений

$k\xi$  по модулю  $p$ , либо, наоборот, для  $\eta$  будем брать первые значения, а для  $\xi$  — наименьшие вычеты произведений —  $k\eta$ . Тогда из отдельных значений  $\xi + \eta i$  соответствующие значения  $x + yi$  находятся по формуле

$$x + yi = \frac{\xi + \eta i}{a - bi} = \frac{a\xi - b\eta}{p} + \frac{a\eta + b\xi}{p} i.$$

Далее, ясно, что когда  $\xi$  увеличивается на единицу,  $\eta$  или возрастает на  $k$ , или уменьшается на  $p - k$ , и потому  $x + yi$  претерпевает либо изменение

$$\frac{a - kb}{p} + \frac{ak + b}{p} i,$$

либо изменение

$$\frac{a - kb}{p} + b + \left( \frac{ak + b}{p} - a \right) i;$$

это замечание служит для облегчения вычислений.

Наконец, если отыскиваются абсолютно наименьшие вычеты, то эти правила меняются лишь в том отношении, что теперь числу  $\xi$  придаются последовательно значения в пределах от  $-\frac{1}{2}p$  до  $+\frac{1}{2}p$ , в то время как для  $\eta$  берутся абсолютно наименьшие вычеты произведений  $k\xi$ . Здесь приводится таблица полученных таким путем наименьших вычетов для модуля  $5 + 2i$ .

Наименьшие вычеты

| $\xi + \eta i$ | $x + yi$ | $\xi + \eta i$ | $x + yi$  | $\xi + \eta i$ | $x + yi$ |
|----------------|----------|----------------|-----------|----------------|----------|
| 0              | 0        | 10 + 25i       | + 5 i     | 20 + 21i       | + 2 + 5i |
| 1 + 17i        | — 1 + 3i | 11 + 13i       | + 1 + 3 i | 21 + 9i        | + 3 + 3i |
| 2 + 5 i        | + i      | 12 + i         | + 2 + i   | 22 + 26i       | + 2 + 6i |
| 3 + 22i        | + 1 + 4i | 13 + 18i       | + 1 + 4 i | 23 + 14i       | + 3 + 4i |
| 4 + 10i        | + 2i     | 14 + 6i        | + 2 + 2 i | 24 + 2i        | + 4 + 2i |
| 5 + 27i        | — 1 + 5i | 15 + 23i       | + 1 + 5 i | 25 + 19i       | + 3 + 5i |
| 6 + 15i        | + 3i     | 16 + 11i       | + 2 + 3 i | 26 + 7i        | + 4 + 3i |
| 7 + 3 i        | + 1 + i  | 17 + 28i       | + 1 + 6 i | 27 + 24i       | + 3 + 6i |
| 8 + 20i        | + 4i     | 18 + 16i       | + 2 + 4 i | 28 + 12i       | + 4 + 4i |
| 9 + 8i         | + 1 + 2i | 19 + 4i        | + 3 + 2 i |                |          |

## Абсолютно наименьшие вычеты

| $\xi + \eta i$ | $x + yi$  | $\xi + \eta i$ | $x + yi$  | $\xi + \eta i$ | $x + yi$  |
|----------------|-----------|----------------|-----------|----------------|-----------|
| $-14 - 6i$     | $-2 - 2i$ | $-4 - 10i$     | $-2i$     | $+5 - 2i$      | $+1$      |
| $-13 + 11i$    | $-3 + i$  | $-3 + 7i$      | $-1 + i$  | $+6 - 14i$     | $+2 - 2i$ |
| $-12 - i$      | $-2 - i$  | $-2 - 5i$      | $-i$      | $+7 + 3i$      | $+1 + i$  |
| $-11 - 13i$    | $-1 - 3i$ | $-1 + 12i$     | $-1 + 2i$ | $+8 - 9i$      | $+2 - i$  |
| $-10 + 4i$     | $-2$      | $0$            | $0$       | $+9 + 8i$      | $+1 + 2i$ |
| $-9 - 8i$      | $-1 - 2i$ | $+1 - 12i$     | $+1 - 2i$ | $+10 - 4i$     | $+2$      |
| $-8 + 9i$      | $-2 + i$  | $+2 + 5i$      | $+i$      | $+11 + 13i$    | $+1 + 3i$ |
| $-7 - 3i$      | $-1 - i$  | $+3 - 7i$      | $+1 - i$  | $+12 + i$      | $+2 + i$  |
| $-6 + 14i$     | $-2 + 2i$ | $+4 + 10i$     | $+2i$     | $+13 - 11i$    | $+3 - i$  |
| $-5 + 2i$      | $-1$      |                |           | $+14 + 6i$     | $+2 + 2i$ |

Второй случай, когда  $a$  и  $b$  не взаимно просты, легко может быть сведен к предыдущему случаю. Пусть  $\lambda$  — наибольший общий делитель чисел  $a$ ,  $b$ , и  $a = \lambda a'$ ,  $b = \lambda b'$ . Обозначим, далее, через  $F$  произвольный наименьший вычет для модуля  $\lambda$ , рассматриваемый как комплексное число, т. е. будем считать, что  $F$  — произвольное число  $x + yi$ , у которого  $x$ ,  $y$  заключены или в границах  $0$  и  $\lambda$ , или в границах  $-\frac{1}{2}\lambda$  и  $+\frac{1}{2}\lambda$  (в зависимости от того, идет ли речь просто о наименьших или об абсолютно наименьших вычетах); наконец, обозначим через  $F'$  произвольный наименьший вычет для модуля  $a' + b'i$ . Тогда  $(a' + b'i)F + F'$  будет некоторым наименьшим вычетом для модуля  $a + bi$ , и мы получим полную систему этих вычетов, если будем комбинировать всевозможные значения  $F$  со всевозможными значениями  $F'$ .

Два комплексных числа называются взаимно простыми, если, кроме единиц, они не обладают другими общими делителями; если же такие общие делители существуют, то наибольшими общими называются те из них, нормы которых наибольшие.



Если даны разложения на простые сомножители двух данных чисел, то нахождение наибольшего общего делителя может быть выполнено точно таким же образом, как и для вещественных чисел («Арифметические исследования», п. 18). Одновременно из этого вытекает, что все общие делители двух данных чисел должны входить также и в найденный таким способом наибольший общий делитель. А так как само собой ясно, что три ассоциированных с ним числа тоже являются общими делителями, то всегда должны называться наибольшими четыре и только четыре общих делителя, и их норма является кратным каждого другого общего делителя.

Если разложение двух данных чисел на простые сомножители не дано, то наибольший общий делитель находится при помощи алгоритма, подобного тому, который используется в случае вещественных чисел. Пусть  $m, m'$  — два заданных числа; последовательным делением образуем ряд чисел  $m'', m''', \dots$ , такой, что  $m''$  является абсолютно наименьшим вычетом числа  $m$  по модулю  $m'$ , число  $m'''$  — абсолютно наименьшим вычетом числа  $m'$  по модулю  $m''$  и т. д. Если нормы чисел  $m, m', m'', m''', \dots$  обозначить соответственно через  $p, p', p'', p''', \dots$ , то  $p''/p'$  будет нормой отношения  $m''/m'$ , и потому, по определению абсолютно наименьшего вычета, будет заведомо не больше чем  $1/2$ ; так же обстоит дело для  $p'''/p''$  и т. д. Поэтому положительные вещественные целые числа  $p', p'', p''', \dots$  будут образовывать непрерывно убывающий ряд, так что в конце концов мы обязательно придем к члену 0, или, что то же самое, в ряду  $m, m', m'', m''', \dots$  в конце концов получится член, который входит в предыдущий член без остатка. Пусть этот член есть  $m^{(n+1)}$  и пусть

$$\begin{aligned} m &= km' + m'', \\ m' &= k'm'' + m''', \\ m'' &= k''m''' + m^{(4)}, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ m^{(n)} &= k^{(n)} m^{(n+1)}. \end{aligned}$$

Если пройти этот ряд равенств в обратном порядке, то мы получим, что  $m^{(n+1)}$  входит во все предшествующие члены  $m^{(n)}, \dots, m'', m', m$ . Если же пройти эти равенства в прямом порядке, то станет

ясно, что каждый общий делитель чисел  $m, m'$  входит также и в каждое последующее число. Первое показывает, что  $m^{(n+1)}$  является общим делителем чисел  $m, m'$ , а второе — что этот делитель наибольший.

Если последний остаток  $m^{(n+1)}$  окажется равным одной из четырех единиц  $1, -1, i, -i$ , то это будет указывать на то, что  $m$  и  $m'$  взаимно просты.

## 47

Если равенства предыдущего пункта, за исключением последнего, скомбинировать между собой так, чтобы  $m'', m''', m''', \dots, m^{(n)}$  исключились, то получается равенство вида

$$m^{(n+1)} = hm + h'm',$$

где  $h$  и  $h'$  являются целыми числами, и притом, если использовать обозначение, введенное в «Арифметических исследованиях», п. 27, выполняются равенства

$$h = \pm [k', k'', k''', \dots, k^{(n-1)}] = \pm [k^{(n-1)}, k^{(n-2)}, \dots, k'', k'],$$

$$h' = \mp [k, k', k'', k''', \dots, k^{(n-1)}] = \mp [k^{(n-1)}, k^{(n-2)}, \dots, k'', k', k],$$

причем берутся верхние или нижние знаки в зависимости от того, четно  $n$  или нечетно. Эту теорему мы выскажем следующим образом.

*Наибольший общий делитель двух комплексных чисел  $m, m'$  может быть представлен в виде  $hm + h'm'$ , где  $h$  и  $h'$  являются целыми числами.*

Очевидно, что это справедливо не только для того наибольшего общего делителя, к которому приводит алгоритм предыдущего пункта, но и для трех с ним ассоциированных, для которых вместо чисел  $h, h'$  нужно брать либо  $hi, h'i$ , либо  $-h, -h'$ , либо  $-hi, -h'i$ .

Если поэтому числа  $m, m'$  взаимно просты, то разрешимо уравнение

$$1 = hm + h'm'.$$

Пусть, например, даны числа  $31 + 6i = m$ ,  $11 - 20i = m'$ . Мы находим здесь

$$\begin{aligned} k &= i, & m'' &= +11 - 5i, \\ k' &= +1 - i, & m''' &= +5 - 4i, \\ k'' &= +2, & m'''' &= +1 + 3i, \\ k''' &= -1 - 2i, & m''''' &= +i, \\ k'''' &= +3 - i, \end{aligned}$$

откуда

$$\begin{aligned} [k', k'', k'''] &= -6 - 5i, \\ [k, k', k'', k'''] &= +4 - 10i, \end{aligned}$$

и потому

$$m''''' = i = (6 + 5i)m + (4 - 10i)m',$$

и

$$1 = (5 - 6i)m + (-10 - 4i)m'.$$

Это равенство легко можно проверить вычислением.

## 48

Изложенным до сих пор подготовлено все, что нужно для теории сравнений первой степени в арифметике комплексных чисел; но так как эта теория не существенно отличается от соответствующей теории в арифметике вещественных чисел, которая исчерпывающе изложена в «Арифметических исследованиях», то будет достаточно отметить здесь только основные моменты.

I. Сравнение  $mt \equiv 1 \pmod{m'}$  эквивалентно неопределенному уравнению  $mt + m'u = 1$ , и если последнее удовлетворяется при значениях  $t = h$ ,  $u = h'$ , то общее решение первого представляется в виде  $t \equiv h \pmod{m'}$ . Условие же разрешимости заключается в том, что модуль  $m'$  не должен иметь с коэффициентом  $m$  общих делителей.

II. Решение сравнения  $ax + b \equiv c \pmod{M}$  в случае, когда  $a$  и  $M$  взаимно просты, зависит от решения сравнения

$$at \equiv 1 \pmod{M},$$

и если второе сравнение удовлетворяется при  $t = h$ , то общее решение первого дается формулой

$$x \equiv (c - b)h \pmod{M}.$$

III. Сравнение  $ax + b \equiv c \pmod{M}$  в случае, когда  $a$  и  $M$  имеют общий делитель  $\lambda$ , эквивалентно сравнению

$$\frac{a}{\lambda}x \equiv \frac{c-b}{\lambda} \pmod{\frac{M}{\lambda}}.$$

Если поэтому за  $\lambda$  взят наибольший общий делитель чисел  $a$  и  $M$ , то решение заданного сравнения сводится к предыдущему случаю, и ясно, что условием, необходимым и достаточным для разрешимости сравнения, является то, что  $\lambda$  входит также и в разность  $c - b$ .

#### 49

До сих пор мы излагали только элементарные вопросы, которые однако, нельзя было опустить, не утратив связности изложения. В более глубоких исследованиях арифметика комплексных чисел оказывается подобной арифметике вещественных чисел в том отношении, что теоремы становятся проще и изящнее, если рассматривать только модули, являющиеся простыми числами; распространение их на составные модули в большинстве случаев скорее длинно, чем трудно, и требует более технической работы, нежели искусства. По этой причине в дальнейшем речь будет идти главным образом о простых модулях.

#### 50

Если  $X$  обозначает функцию от переменной  $x$  вида

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \dots + Mx + N,$$

где  $n$  — вещественное положительное целое число,  $A, B, C, \dots$  — вещественные или мнимые целые числа, и если  $m$  есть целое комплексное число, то мы также и здесь будем называть **корнем сравнения**  $X \equiv 0 \pmod{m}$  каждое целое число, которое, будучи подставлено вместо  $x$ , даст делящееся на модуль  $m$  значение функции  $X$ .

Решения при помощи корней, которые сравнимы по модулю, мы не будем рассматривать как различные.

Если модуль является простым числом, то такое сравнение степени  $n$  также и здесь не может иметь больше чем  $n$  различных решений. Если  $\alpha$  обозначает любое определенное (комплексное) целое число, то  $X$  посредством деления на  $x - \alpha$  может быть представлена в виде  $X = (x - \alpha) X' + h$ , где  $h$  будет определенным целым числом, а  $X'$  — функцией  $(n - 1)$ -й степени с целочисленными коэффициентами. Если теперь  $\alpha$  — корень сравнения  $X \equiv 0 \pmod{m}$ , то  $h$ , очевидно, будет делиться на  $m$ , т. е. для каждого значения переменной  $x$  будет выполняться сравнение  $X \equiv (x - \alpha) X' \pmod{m}$ .

Точно так же, если  $\beta$  обозначает некоторое определенное целое число, то  $X'$  приводится к виду  $(x - \beta) X'' + h'$ , где  $X''$  является функцией  $(n - 2)$ -й степени с целочисленными коэффициентами. Если же мы предположим, что число  $\beta$  является корнем сравнения  $X \equiv 0$ , то оно должно также удовлетворять сравнению  $(\beta - \alpha) X' \equiv 0$ , а, значит, и сравнению  $X' \equiv 0$ , если корни  $\alpha, \beta$  не сравнимы между собой, откуда мы заключаем, что также и  $h'$  должно делиться на  $m$ , т. е. что должно быть  $X \equiv (x - \alpha)(x - \beta) X'' \pmod{m}$  при всех значениях  $x$ .

Аналогичным образом, если имеется третий не сравнимый с двумя первыми корень  $\gamma$ , мы получаем, что  $X \equiv (x - \alpha)(x - \beta)(x - \gamma) X'''$ , где  $X'''$  является функцией  $(n - 3)$ -й степени с целочисленными коэффициентами. Подобным же образом можно продолжать и дальше, и, кроме того, ясно, что коэффициент старшего члена у каждой функции будет равен числу  $A$ , которое мы можем предполагать не делящимся на  $m$ , так как иначе сравнение  $X \equiv 0$  по существу имело бы меньшую степень. Если поэтому имеется  $n$  не сравнимых между собой корней, именно,  $\alpha, \beta, \gamma, \dots, \nu$ , то при всех значениях  $x$  выполняется сравнение

$$X \equiv A (x - \alpha)(x - \beta)(x - \gamma) \dots (x - \nu) \pmod{m};$$

следовательно, подстановка каждого нового не сравнимого ни с одной из величин  $\alpha, \beta, \gamma, \dots, \nu$  значения будет давать для  $X$  значение, не делящееся на  $m$ , откуда и следует справедливость нашей теоремы.

Впрочем, это доказательство по существу совпадает с тем, которое мы провели в п. 43 «Арифметических исследований», отдельные моменты которого имеют силу для комплексных чисел так же, как и для вещественных.

## 5f

То, что в третьем разделе «Арифметических исследований» говорилось относительно степенных вычетов, с незначительными изменениями сохраняет силу также и в арифметике комплексных чисел; в большинстве случаев могут быть сохранены даже доказательства теорем. Однако, для того чтобы ничего не пропускать, мы хотим привести основные теоремы, снабженные краткими доказательствами, причем все время будет подразумеваться, что модуль является простым числом.

**Теорема.** Если  $k$  обозначает целое число, не делящееся на модуль  $m$ , норма которого равна  $p$ , то  $k^{p-1} \equiv 1 \pmod{m}$ .

**Доказательство.** Пусть  $a, b, c, \dots$  образуют полную систему не-сравнимых между собой вычетов по модулю  $m$ , из которой, однако, выброшен вычет, делящийся на  $m$ , так что количество этих чисел, совокупность которых мы обозначим через  $S$ , равно  $p-1$ . Пусть, далее,  $S'$  — совокупность произведений  $ka, kb, kc, \dots$ . По предположению ни одно из этих произведений не делится на  $m$ , и потому каждое из них имеет сравнимый с ним вычет в совокупности  $S$ , так что можно положить  $ak \equiv a', bk \equiv b', ck \equiv c', \dots \pmod{m}$ , где числа  $a', b', c', \dots$  содержатся в совокупности  $S$ . Совокупность чисел  $a', b', c', \dots$  мы обозначим через  $S''$ . Пусть, далее,  $P, P', P''$  являются произведениями отдельных чисел совокупностей  $S, S', S''$ , т. е.

$$P = abc\dots,$$

$$P' = k^{p-1}abc\dots = k^{p-1}P,$$

$$P'' = a'b'c'\dots$$

Так как числа совокупности  $S''$  последовательно сравнимы с числами совокупности  $S'$ , то  $P'' \equiv P'$  или  $P'' \equiv k^{p-1}P$ . Но так как легко видеть, что каждые два числа совокупности  $S''$  не-сравнимы,

и потому все они различны между собой, то числа совокупности  $C''$  обязательно будут совпадать с числами совокупности  $C$ , только взятыми в измененном порядке, и потому  $P'' = P$ . Следовательно, число  $(k^{p-1} - 1)P$  делится на  $m$ , для чего необходимо, так как  $m$  является простым числом, не входящим в отдельные делители числа  $P$ , чтобы  $k^{p-1} - 1$  делилось на  $m$ .

## 25

**Теорема.** Если, как и в предыдущем пункте,  $k$  обозначает целое число, не делящееся на модуль  $m$ , а  $t$  — наименьший показатель (не считая нуля), для которого  $k^t \equiv 1 \pmod{m}$ , то  $t$  является делителем всякого другого показателя  $u$ , для которого  $k^u \equiv 1 \pmod{m}$ .

**Доказательство.** Если предположить, что  $t$  не является делителем числа  $u$ , то пусть  $gt$  будет кратностью числа  $t$ , которая является первой, большей чем  $u$ , так что  $gt - u$  есть целое положительное число, меньшее чем  $t$ . Из  $k^t \equiv 1$ ,  $k^u \equiv 1$  следует, что  $0 \equiv k^{gt} - k^u \equiv k^u (k^{gt-u} - 1)$ , и потому  $k^{gt-u} \equiv 1$  т. е. существует степень числа  $k$  с показателем, меньшим чем  $t$ , которая сравнима с единицей. Но это противоречит предположению.

Как следствие отсюда вытекает, что  $t$  заведомо делит  $p - 1$ .

Такие числа  $t$ , для которых  $t = p - 1$ , мы будем и здесь называть первообразными корнями по модулю  $m$ . Сейчас мы покажем, что они действительно существуют.

## 53

Разложим число  $p - 1$  на его простые сомножители:

$$p - 1 = a^\alpha b^\beta c^\gamma \dots,$$

где  $a, b, c, \dots$  обозначают различные между собой положительные вещественные простые числа. Пусть, далее,  $A, B, C, \dots$  — целые (комплексные) не делящиеся на  $m$  числа, которые не удовлетворяют соответственно сравнениям

$$x^{(p-1)/a} \equiv 1, x^{(p-1)/b} \equiv 1, x^{(p-1)/c} \equiv 1, \dots;$$

то, что такие числа существуют, очевидно на основании теоремы п. 50. Наконец, пусть  $h$  сравнимо по модулю  $t$  с произведением

$$A^{(p-1)/a^\alpha} \cdot B^{(p-1)/b^\beta} \cdot C^{(p-1)/c^\gamma} \dots$$

Тогда я утверждаю, что  $h$  является первообразным корнем.

**Доказательство.** Если обозначить через  $t$  показатель наинизшей сравнимой с единицей степени  $h^t$ , то из предположения, что  $h$  не является первообразным корнем, следовало бы, что  $t$  является делителем числа  $p-1$ , т. е. что число  $(p-1)/t$  было целым, большим чем 1 числом.

Очевидно, что вещественные простые сомножители этого целого числа содержатся среди чисел  $a, b, c, \dots$ . Предположим поэтому (что допустимо), что  $(p-1)/t$  делится на  $a$  и положим  $p-1 = atu$ . Вследствие того, что  $h^t \equiv 1$ , тогда также и  $h^{tu} \equiv 1$ , т. е.

$$A^{\frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} \cdot B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} \cdot C^{\frac{p-1}{c^\gamma} \cdot \frac{p-1}{a}} \dots \equiv 1.$$

Но очевидно, что  $(p-1)/ab^\beta$  является целым числом, и потому

$$B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} = (B^{p-1})^{(p-1)/ab^\beta} \equiv 1,$$

так же, как

$$C^{\frac{p-1}{c^\gamma} \cdot \frac{p-1}{a}} \equiv 1,$$

и т. д. Поэтому должно быть

$$A^{\frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} \equiv 1.$$

Выберем теперь такое положительное целое число  $\lambda$ , что

$$\lambda b^\beta c^\gamma \dots \equiv 1 \pmod{a},$$

что возможно, ибо простое число  $a$  не входит делителем в число  $b^\beta c^\gamma \dots$ , и положим  $\lambda b^\beta c^\gamma \dots = 1 + a\mu$ . Тогда, очевидно, будет выпол-

$$\begin{aligned} & \text{няться сравнение } A^{\lambda \frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} \equiv 1, \text{ или, так как } \lambda \cdot \frac{p-1}{a^\alpha} \cdot \frac{p-1}{a} = \\ & = (1 + a\mu) \frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}, \end{aligned}$$



$$A^{(p-1)\mu} \cdot A^{\frac{p-1}{a}} \equiv 1,$$

откуда следует, так как  $A^{(p-1)\mu} \equiv 1$ , что и  $A^{(p-1)/a} \equiv 1$ , а это противоречит предположению. Следовательно, предположение о том, что  $t$  является делителем числа  $p-1$ , не может быть справедливым, и потому  $h$  обязательно является первообразным корнем.

54

Если  $h$  обозначает первообразный корень по модулю  $m$ , норма которого равна  $p$ , то члены ряда

$$1, h, h^2, h^3, \dots, h^{p-2}$$

будут попарно несравнимы между собой, откуда легко следует, что каждое целое число, не делящееся на модуль, должно быть сравнимо с одним из указанных чисел, т. е. что этот ряд представляет полную систему несравнимых вычетов, за исключением нуля. *Показатель той степени, с которой сравнимо заданное число, может быть назван индексом этого числа, если  $h$  рассматривается как основание.* Мы приведем сейчас несколько примеров, причем рядом с каждым индексом будет указываться абсолютно наименьший вычет.

### Первый пример

$$m = 5 + 4i, \quad p = 41, \quad h = 1 + 2i$$

| Индекс | Вычет | Индекс | Вычет | Индекс | Вычет | Индекс | Вычет | Индекс | Вычет |
|--------|-------|--------|-------|--------|-------|--------|-------|--------|-------|
| 0      | +1    | 8      | —4    | 16     | —2+2i | 24     | +2i   | 32     | +1+i  |
| 1      | +1+2i | 9      | —3+i  | 17     | —1+2i | 25     | —3i   | 33     | +1+3i |
| 2      | +1—i  | 10     | —i    | 18     | +4i   | 26     | +2+2i | 34     | +2    |
| 3      | +3+i  | 11     | +2—i  | 19     | +1+3i | 27     | +2+i  | 35     | —3    |
| 4      | —2i   | 12     | —1—i  | 20     | —1    | 28     | +4    | 36     | +2—2i |
| 5      | +3i   | 13     | +1—3i | 21     | —1—2i | 29     | +3—i  | 37     | +1—2i |
| 6      | —2—2i | 14     | —2    | 22     | —1+i  | 30     | +i    | 38     | —4i   |
| 7      | —2—i  | 15     | +3    | 23     | —3—i  | 31     | —2+i  | 39     | —1—3i |

## Второй пример

$$m = 7, \quad p = 49, \quad h = 1 + 2i$$

| Индекс | Вычет    | Индекс | Вычет    | Индекс | Вычет    | Индекс | Вычет    | Индекс | Вычет    |
|--------|----------|--------|----------|--------|----------|--------|----------|--------|----------|
| 0      | + 1      | 10     | — 1 — i  | 20     | + 2i     | 30     | + 2 — 2i | 40     | + 3      |
| 1      | + 1 + 2i | 11     | + 1 — 3i | 21     | + 3 + 2i | 31     | — 1 + 2i | 41     | + 3 — i  |
| 2      | — 3 — 3i | 12     | — i      | 22     | — 1 + i  | 32     | + 2      | 42     | — 2 — 2i |
| 3      | + 3 — 2i | 13     | + 2 — i  | 23     | — 3 — i  | 33     | + 2 — 3i | 43     | + 2 + i  |
| 4      | — 3i     | 14     | — 3 + 3i | 24     | — 1      | 34     | + 1 + i  | 44     | — 2i     |
| 5      | — 1 — 3i | 15     | — 2 — 3i | 25     | — 1 — 2i | 35     | — 1 + 3i | 45     | — 3 — 2i |
| 6      | — 2 + 2i | 16     | — 3      | 26     | + 3 + 3i | 36     | + i      | 46     | + 1 — i  |
| 7      | + 1 — 2i | 17     | — 3 + i  | 27     | — 3 + 2i | 37     | — 2 + i  | 47     | + 3 + i  |
| 8      | — 2      | 18     | + 2 + 2i | 28     | + 3i     | 38     | + 3 — 3i |        |          |
| 9      | — 2 + 3i | 19     | — 2 — i  | 29     | + 1 + 3i | 39     | + 2 + 3i |        |          |

Относительно первообразных корней и алгоритма индексов мы добавим еще некоторые замечания, однако доказательства, вследствие их легкости, опустим.

I. В заданной системе индексы, сравнимые по модулю  $p - 1$ , соответствуют вычетам, сравнимым по модулю  $m$ , и обратно.

II. Вычеты, соответствующие индексам, взаимно простым с числом  $p - 1$ , тоже являются первообразными корнями, и обратно.

III. Если  $t$  является индексом первообразного корня  $h'$ , когда за основание взят первообразный корень  $h$ , и наоборот,  $t'$  является индексом числа  $h$ , когда за основание взято число  $h'$ , то  $tt' \equiv 1 \pmod{p-1}$ ; и если при тех же предположениях индексы какого-нибудь другого числа в этих двух системах равны соответственно  $u$  и  $u'$ , то  $tu' \equiv u$ ,  $t'u \equiv u' \pmod{p-1}$ .

IV. Если числа  $1$ ,  $1 + i$  и ассоциированные с ними исключить (как слишком тривиальные) из числа рассматриваемых модулей, то останутся те простые числа, которые в п. 34 были указаны под

рубриками 3 и 4. Нормами последних являются вещественные простые числа вида  $4n + 1$ , нормами же первых — квадраты нечетных вещественных простых чисел; таким образом, в обоих случаях  $p - 1$  делится на 4.

V. Если обозначить индекс числа  $-1$  через  $u$ , то  $2u \equiv 0 \pmod{p-1}$  и потому либо  $u \equiv 0$ , либо  $u \equiv \frac{1}{2}(p-1)$ . Но так как индекс 0 соответствует вычету  $+1$ , то индекс числа  $-1$  обязательно должен быть равен  $\frac{1}{2}(p-1)$ .

VI. Если точно так же обозначить через  $u$  индекс числа  $i$ , то будет выполняться сравнение  $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$ , и потому либо  $u \equiv \frac{1}{4}(p-1)$ , либо  $u \equiv \frac{3}{4}(p-1)$ . Какая из этих двух возможностей осуществляется в действительности, зависит от выбора первообразного корня. Именно, если для взятого в качестве основания первообразного корня  $h$  индекс числа  $i$  равен  $\frac{1}{4}(p-1)$ , то индекс будет равен  $\frac{3}{4}(p-1)$ , когда за основание берется число  $h^\mu$ , где  $\mu$  обозначает положительное, взаимно простое с  $p-1$  целое число вида  $4n + 3$  (например, само число  $p-2$ ), и обратно. Поэтому одна половина первообразных корней дает для числа  $i$  индекс  $\frac{1}{4}(p-1)$ , а другая половина — индекс  $\frac{3}{4}(p-1)$ , и очевидно, что число  $-i$  будет для первых оснований обладать индексом  $\frac{3}{4}(p-1)$ , а для вторых — индексом  $\frac{1}{4}(p-1)$ .

VII. Если модулем является положительное вещественное простое число вида  $4n + 3$ , например, равное  $q$ , так что  $p = q^2$ , то индексы всех вещественных чисел будут делиться на  $q + 1$ . Действительно, если  $t$  обозначает индекс вещественного числа  $k$ , то в силу соотношения  $k^{q-1} \equiv 1 \pmod{q}$  выполняется сравнение  $(q-1)t \equiv 0 \pmod{q^2-1}$ , и потому число  $t/(q+1)$  является целым. Точно так же индексы чисто мнимых чисел вида  $ki$  делятся на  $(q+1)/2$ . Поэтому очевидно, что первообразные корни для таких модулей следует искать только среди смешанных мнимых чисел.

VIII. Напротив, для модуля  $m$ , являющегося смешанным комплексным простым числом (нормой которого, следовательно, служит вещественное простое число вида  $4n + 1$ ), любые первообразные корни могут быть выбраны среди вещественных чисел, так как среди них можно найти даже полную систему несравнимых вычетов (п. 40). Но очевидно, что каждое вещественное число, которое является первообразным корнем по комплексному модулю  $m$ , будет одновременно и первообразным корнем по модулю  $p$  в арифметике вещественных чисел, и обратно.

## 56

*Хотя теория квадратичных вычетов и невычетов для арифметики комплексных чисел содержится в теории биквадратичных вычетов, мы, однако, прежде чем перейти к последней, отдельно приведем здесь основные теоремы первой теории; но при этом ради краткости мы будем говорить только об основном случае, когда модуль является комплексным (нечетным) простым числом.*

Пусть  $m$  — такой модуль, и  $p$  — его норма. Очевидно, что всякое целое (и, как здесь все время будет предполагаться, не делящееся на  $m$ ) число может или не может быть сравнимо по модулю  $m$  с некоторым квадратом в зависимости от того, четным или нечетным будет его индекс, если за основание взять произвольный первообразный корень; в первом случае это целое число называется квадратичным вычетом, а во втором — квадратичным невычетом по модулю  $m$ . Отсюда следует, что среди  $p - 1$  чисел, представляющих полную систему несравнимых (не делящихся на  $m$ ) вычетов, половина будет относиться к квадратичным вычетам, а половина — к квадратичным невычетам. Всякое же другое число, не содержащееся в этой системе, имеет в этом отношении тот же характер, что и сравнимое с ним число системы.

Далее, отсюда следует, что произведение двух квадратичных вычетов, так же, как и произведение двух квадратичных невычетов, является квадратичным вычетом, а произведение квадратичного вычета на квадратичный невычет — квадратичным невычетом; и вообще, произведение любого числа сомножителей будет квадратичным

вычетом или невычетом в зависимости от того, четно или нечетно число невычетов среди этих сомножителей.

Для того чтобы различать квадратичные вычеты от квадратичных невычетов, мы сразу получаем следующий общий критерий.

Число  $k$ , не делящееся на модуль, является по нему квадратичным вычетом или невычетом в зависимости от того, имеет ли место  $k^{(p-1)/2} \equiv -1$  или  $k^{(p-1)/2} \equiv -1 \pmod{m}$ .

Справедливость этой теоремы немедленно следует из того, что при выборе за основание произвольного первообразного корня индекса степени  $k^{(p-1)/2}$  будет или  $\equiv 0$ , или  $\equiv \frac{1}{2}(p-1)$ , смотря по тому, четен или нечетен индекс числа  $k$ .

## 57

Итак, для заданного модуля легко разбить полную систему не-сравнимых вычетов на два класса, именно, на квадратичные вычеты и невычеты, чем одновременно определяется, к каким классам относятся и все остальные числа; однако намного труднее вопрос о критериях, при помощи которых те модули, по которым заданное число является квадратичным вычетом, можно отличать от модулей, по которым оно является невычетом.

Что касается вещественных единиц  $+1$  и  $-1$ , то они в арифметике комплексных чисел сами являются квадратами, а потому и квадратичными вычетами по *каждому* модулю. Точно так же из критерия предыдущего пункта легко видеть, что число  $i$  (а также и  $-i$ ) является квадратичным вычетом по каждому модулю, норма которого  $p$  имеет вид  $8n + 1$ , и невычетом по каждому модулю, норма которого имеет вид  $8n + 5$ . Так как, очевидно, безразлично, брать ли за модуль число  $m$  или одно из ассоциированных с ним чисел  $it, -m, -it$ , то можно считать, что модулем является первичное число среди ассоциированных (п. 36, II), т. е., что если модуль равен  $a + bi$ , то  $a$  нечетно, а  $b$  четно. Так как вследствие этого всегда  $a^2 \equiv 1 \pmod{8}$ , а  $b^2$  или  $\equiv 0$ , или  $\equiv 4 \pmod{8}$ , в зависимости от того, делится  $b$  на 4, или не делится, то числа  $+i$  и  $-i$  будут, очевидно, в первом случае квадратичными вычетами, а во втором — квадратичными невычетами по модулю  $a + bi$ .

Так как вопрос о характере составного числа, т. е. о том, является ли оно квадратичным вычетом или невычетом, сводится к вопросу о характерах сомножителей, то очевидно достаточно ограничиться выводом критериев для отличия тех модулей, по которым заданное число  $k$  является квадратичным вычетом, от тех, по которым оно является квадратичным невычетом, для тех значений  $k$ , которые являются простыми числами и, кроме того,— первичными среди ассоциированных с ними. При этом индуктивное рассмотрение тотчас же дает нам очень изящные теоремы.

Если начать с числа  $1 + i$ , то мы найдем, что оно является квадратичным вычетом по модулям

$$\begin{aligned} & -1 + 2i, \quad +3 - 2i, \quad -5 - 2i, \quad -1 - 6i, \quad +5 + 4i, \\ & +5 - 4i, \quad -7, \quad +7 + 2i, \quad -5 + 6i, \dots, \end{aligned}$$

и, напротив, квадратичным невычетом по модулям

$$\begin{aligned} & -1 - 2i, \quad -3, \quad +3 + 2i, \quad +1 + 4i, \quad +1 - 4i, \quad -5 + 2i, \quad -1 + 6i, \quad +7 - 2i, \\ & -5 - 6i, \quad -3 + 8i, \quad -3 - 8i, \quad +5 + 8i, \quad +5 - 8i, \quad +9 + 4i, \quad +9 - 4i, \dots \end{aligned}$$

Если мы внимательно рассмотрим этот обзор, при котором из каждых четырех ассоциированных модулей мы все время брали первичный, то мы легко заметим, что все модули  $a + bi$  в первом классе обладают тем свойством, что для них  $a + b \equiv +1 \pmod{8}$ , а во втором классе—тем свойством, что для них  $a + b \equiv -3 \pmod{8}$ . Очевидно, что если вместо первичного модуля  $m$  брать ассоциированный с ним модуль  $-m$ , то этот критерий нужно будет изменить таким образом, что для модулей первого класса  $a + b \equiv -1$ , а для модулей второго класса  $a + b \equiv +3 \pmod{8}$ . Поэтому, если наше индуктивное заключение верно, и если  $a + bi$  обозначает простое число, для которого  $a$  нечетно, а  $b$  четно, то вообще  $1 + i$  будет квадратичным вычетом или невычетом по нему в зависимости от того, имеет ли место  $a + b \equiv \pm 1$  или  $\equiv \pm 3 \pmod{8}$ .

Для числа  $-1 - i$  выполняется то же правило, что и для  $1 + i$ . Если же число  $1 - i$  рассматривать как произведение чисел  $-i$  и  $1 + i$ , то ясно, что число  $1 - i$  имеет тот же характер, что и  $1 + i$ , если  $b$  делится на 4, и противоположный, если  $b$  не делится на 4, откуда легко видеть, что  $1 - i$  является квадратичным вычетом по простому числу  $a + bi$ , если  $a - b \equiv \pm 1$ , и квадратичным невычетом, если  $a - b \equiv \pm 3 \pmod{8}$ , все время в предположении, что  $a$  нечетно, а  $b$  четно.

Впрочем, эта вторая теорема может быть выведена из первой также и при помощи одной *более общей теоремы*, которую мы выскажем следующим образом.

*В теории квадратичных вычетов характер числа  $\alpha + \beta i$  по отношению к модулю  $a + bi$  тот же, что и характер числа  $\alpha - \beta i$  по отношению к модулю  $a - bi$ .*

Доказательство этой теоремы получается из того, что оба модуля имеют одну и ту же норму  $p$ , и из того, что если  $(\alpha + \beta i)^{(p-1)/2} - 1$  делится на  $a + bi$ , то и  $(\alpha - \beta i)^{(p-1)/2} - 1$  делится на  $a - bi$ , а если  $(\alpha + \beta i)^{(p-1)/2} + 1$  делится на  $a + bi$ , то и  $(\alpha - \beta i)^{(p-1)/2} + 1$  должно делиться на  $a - bi$ .

## 59

*Теперь мы переходим к другим нечетным простым числам.*

Мы находим, что число  $-1 + 2i$  является квадратичным вычетом по модулям

$$+3 + 2i, +1 - 4i, -5 + 2i, -5 - 2i, -1 - 6i, +7 - 2i, \\ -3 + 8i, +5 + 8i, +5 - 8i, +9 + 4i, \dots,$$

и квадратичным невычетом по модулям

$$-1 - 2i, -3, +3 - 2i, +1 + 4i, -1 + 6i, +5 + 4i, +5 - 4i, \\ -7, +7 + 2i, -5 + 6i, -5 - 6i, -3 - 8i, +9 - 4i, \dots$$

Если привести модули первого класса к их абсолютно наименьшим вычетам по модулю  $-1 + 2i$ , то мы получим только вычеты  $+1$

и  $-1$ ; именно,  $+3+2i \equiv -1$ ,  $+1-4i \equiv -1$ ,  $-5+2i \equiv +1$ ,  $-5-2i \equiv -1$ , и т. д.

С другой стороны, мы находим, что все модули второго класса по модулю  $-1+2i$  или  $\equiv +i$ , или  $\equiv -i$ .

Но  $+1$  и  $-1$  сами являются квадратичными вычетами по модулю  $-1+2i$ , а  $+i$  и  $-i$  — квадратичными невычетами по нему. Поэтому, если верить индуктивному заключению, то получается следующая теорема.

Число  $-1+2i$  является квадратичным вычетом или невычетом по простому числу  $a+bi$  в зависимости от того, будет ли последнее квадратичным вычетом или невычетом по числу  $-1+2i$ , в предположении, что  $a+bi$  является первичным среди четырех ассоциированных чисел, или, точнее, что  $a$  нечетно, а  $b$  четно.

Далее, из этой теоремы немедленно вытекают аналогичные теоремы относительно чисел  $+1-2i$ ,  $-1-2i$ ,  $+1+2i$ .

## 60

Если мы проведем подобное же индуктивное исследование относительно числа  $-3$  или  $+3$ , то найдем, что каждое из них является квадратичным вычетом по модулям

$$+3+2i, +3-2i, -1+6i, -1-6i, -7, -5+6i, \\ -5-6i, -3+8i, -3-8i, +9+4i, +9-4i, \dots,$$

и квадратичным невычетом по модулям

$$-1+2i, -1-2i, +1+4i, +1-4i, -5+2i, -5-2i, \\ +5+4i, +5-4i, +7+2i, +7-2i, +5+8i, +5-8i, \dots$$

Первые сравнимы по модулю 3 с одним из четырех чисел  $+1$ ,  $-1$ ,  $+i$ ,  $-i$ , вторые же — с одним из четырех чисел  $+1+i$ ,  $+1-i$ ,  $-1+i$ ,  $-1-i$ . Первые сами являются квадратичными вычетами, последние же — квадратичными невычетами по модулю 3.



Поэтому наша индукция показывает, что простое число  $a + bi$  (все время в предположении, что  $a$  нечетно, а  $b$  четно) так же относится к числу  $-3$  (и к числу  $+3$ ), как второе относится к первому (имеется в виду вопрос о том, является ли одно число квадратичным вычетом или невычетом другого).

Если подобным же индуктивным способом рассмотреть другие простые числа, то везде мы обнаружим этот в высшей степени изящный закон взаимности и придем, таким образом, к следующей фундаментальной теореме относительно квадратичных вычетов в арифметике комплексных чисел.

*Если  $a + bi$ ,  $A + Bi$  обозначают простые числа с тем свойством, что  $a$ ,  $A$  нечетны, а  $b$ ,  $B$  четны, то или каждое из этих чисел будет квадратичным вычетом по другому, или каждое — квадратичным невычетом.*

Несмотря на исключительную простоту этой теоремы, доказательство ее представляет очень большие трудности, на которых мы, однако, не будем здесь задерживаться, так как сама теорема является лишь частным случаем более общей теоремы, которая содержит в себе всю теорию биквадратичных вычетов. К ней мы поэтому теперь и переходим.

## 61

То, что в п. 2 сочинения первого говорилось относительно понятий биквадратичного вычета и невычета, мы перенесем также и на арифметику комплексных величин, причем, как и раньше, ограничимся рассмотрением модулей, являющихся простыми числами; одновременно, в большинстве случаев без особого упоминания, будет предполагаться, что за модуль берется первичное среди ассоциированных чисел, т. е. число, сравнимое с 1 по модулю  $2+2i$ , и, кроме того, что числа, о характерах которых (т. е. о том, являются ли они биквадратичными вычетами или невычетами) идет речь, не делятся на модуль.

Для заданного модуля не делящиеся на него числа можно было бы разбить на три класса, первый из которых содержал бы биквадратичные вычеты, второй — те биквадратичные невычеты, которые являются квадратичными вычетами, и третий — квадратичные

невычеты. Однако нам будет удобнее разбить третий из этих классов на два, так что всего получится четыре класса.

Если взять за основание какой-нибудь первообразный корень, то биквадратичные вычеты будут иметь индексы, делящиеся на 4, т. е. имеющие вид  $4n$ ; те невычеты, которые являются квадратичными вычетами, будут иметь индексы вида  $4n + 2$ ; наконец, среди квадратичных невычетов часть будет иметь индексы вида  $4n + 1$ , а часть — индексы вида  $4n + 3$ . Таким образом, действительно получаются четыре класса; однако различие между двумя последними классами является не абсолютным, а зависит от первообразного корня, выбранного за основание; действительно, легко видеть, что для одной половины первообразных корней заданный квадратичный невычет имеет индекс вида  $4n + 1$ , а для другой половины — индекс вида  $4n + 3$ . Чтобы избежать этой неопределенности, мы будем предполагать, что всегда выбирается такой первообразный корень, для которого индекс  $(p-1)/4$  принадлежит числу  $+i$  (ср. п. 55, VI). Таким образом, получается *разбиение на классы*, которое без помощи первообразных корней можно более коротко описать следующим образом.

*Первый* класс содержит те числа  $k$ , для которых  $k^{(p-1)/4} \equiv 1$ ; эти числа являются биквадратичными вычетами по модулю.

*Второй* класс содержит те числа, для которых  $k^{(p-1)/4} \equiv i$ .

*Третий* класс содержит те числа, для которых  $k^{(p-1)/4} \equiv -1$ .

*Четвертый* класс содержит те числа, для которых  $k^{(p-1)/4} \equiv -i$ .

Третий класс будет содержать биквадратичные невычеты, являющиеся квадратичными вычетами; на второй и четвертый классы подразделяются квадратичные невычеты.

Числам этих классов мы будем сопоставлять соответственно биквадратичные характеры 0, 1, 2, 3. Если мы определим характер  $\lambda$  числа  $k$  по модулю  $m$  так, что он должен совпадать с показателем той степени числа  $i$ , с которой сравнимо число  $k^{(p-1)/4}$ , то очевидно, что характеры, сравнимые по модулю 4, следует рассматривать как эквивалентные. Впрочем, пока это понятие вводится только для модулей, являющихся простыми числами; в продолжении этих исследований мы покажем, как его можно обобщить и на составные модули.

Чтобы можно было легче прийти к индуктивному заключению относительно характеров модулей, мы даем объемистую таблицу, при помощи которой можно будет сравнительно легко найти характер любого заданного числа по отношению к модулю, норма которого не больше чем 157, если иметь в виду следующие замечания.

Так как характер составного числа равен (или сравним по модулю 4) сумме характеров отдельных сомножителей, то достаточно уметь определять для заданного модуля характеры простых чисел. Так как, далее, характеры единиц  $-1$ ,  $+i$ ,  $-i$ , очевидно, сравнимы по модулю 4 соответственно с числами  $(p-1)/2$ ,  $(p-1)/4$ ,  $3(p-1)/4$ , то будет достаточно указать характеры только первичных чисел среди ассоциированных. Так как, наконец, числа, сравнимые по модулю  $m$ , имеют один и тот же характер, то достаточно занести в таблицу характеры тех чисел, которые содержатся в системе абсолютно наименьших вычетов. Кроме того, при помощи рассуждений, аналогичных рассуждениям п. 58, можно доказать, что если для модуля  $a + bi$  характер числа  $A + Bi$  равен  $\lambda$ , а для модуля  $a - bi$  характером числа  $A - Bi$  является  $\lambda'$ , то всегда  $\lambda \equiv -\lambda' \pmod{4}$ , т. е.  $\lambda + \lambda'$  делится на 4; поэтому в таблице нужно помещать только те модули, у которых  $b$  или равно 0, или положительно.

Если, например, отыскивается характер числа  $11 - 6i$  по отношению к модулю  $-5 - 6i$ , то вместо этих чисел мы подставляем числа  $11 + 6i$  и  $-5 + 6i$ ; затем определяем (п. 43) абсолютно наименьший вычет числа  $11 + 6i$  по модулю  $-5 + 6i$ , который оказывается равным  $-1 - 4i = -1 \cdot (1 + 4i)$ . Поэтому, так как для модуля  $-5 + 6i$  характер числа  $-1$  равен 30, а характер числа  $1 + 4i$ , согласно таблице, равен 2, то число 32 (или 0) будет характером числа  $11 + 6i$  для модуля  $-5 + 6i$ , а потому, согласно последнему замечанию, также и характером числа  $11 - 6i$  для модуля  $-5 - 6i$ . Точно так же, если отыскивается характер числа  $-5 + 6i$  по отношению к модулю  $11 + 6i$ , то абсолютно наименьший вычет первого, равный  $1 - 5i$ , разлагается на сомножители  $-i$ ,  $1 + i$ ,  $3 - 2i$ , которым соответствуют характеры 117, 0, 1, так что искомый характер равен 118 или 2; такой же характер имеет и число  $-5 - 6i$  по отношению к модулю  $11 - 6i$ .

| Модуль    | Характер         | Числа                                                                     |
|-----------|------------------|---------------------------------------------------------------------------|
| $-3$      | 3                | $1 + i$                                                                   |
| $+3 + 2i$ | 3                | $1 + i$                                                                   |
| $+1 + 4i$ | 1<br>3           | $-1 + 2i$<br>$1 + i$                                                      |
| $-5 + 2i$ | 0<br>1<br>2      | $-1 - 2i$<br>$1 + i$<br>$-1 + 2i$                                         |
| $-1 + 6i$ | 0<br>1<br>2      | $-3$<br>$1 + i, -1 + 2i$<br>$-1 - 2i$                                     |
| $+5 + 4i$ | 0<br>1<br>3      | $1 + i$<br>$-3$<br>$-1 + 2i, -1 - 2i$                                     |
| $-7$      | 0<br>1<br>2<br>3 | $-3$<br>$-1 + 2i, 3 - 2i$<br>$1 + i$<br>$-1 - 2i, 3 + 2i$                 |
| $+7 + 2i$ | 0<br>1<br>2<br>3 | $1 + i, 3 + 2i, 3 - 2i, 1 - 4i$<br>$-3$<br>$-1 - 2i, 1 + 4i$<br>$-1 + 2i$ |
| $-5 + 6i$ | 0<br>1<br>2<br>3 | $1 + i, -3, 3 + 2i, 3 - 2i$<br>$1 - 4i$<br>$1 + 4i$<br>$-1 + 2i, -1 - 2i$ |

| Модуль     | Характер         | Числа                                                                                                             |
|------------|------------------|-------------------------------------------------------------------------------------------------------------------|
| $-3 + 8i$  | 0<br>1<br>2<br>3 | $-1 + 2i, 3 - 2i, 1 - 4i$<br>$1 + i, 3 + 2i$<br>$-3$<br>$-1 - 2i, 1 + 4i, -5 + 2i$                                |
| $+5 + 8i$  | 0<br>1<br>2<br>3 | $-1 - 2i$<br>$-5 - 2i, -1 + 6i$<br>$-1 + 2i, 3 - 2i$<br>$1 + i, -3, 3 + 2i, 1 + 4i, 1 - 4i$                       |
| $+9 + 4i$  | 0<br>1<br>2<br>3 | $-1 + 2i, 3 + 2i$<br>$1 + i, -1 - 2i, 3 - 2i$<br>$-3, 1 + 4i$<br>$1 - 4i, -5 + 2i$                                |
| $-1 + 10i$ | 0<br>1<br>2<br>3 | $1 + i, -1 + 2i, -1 - 2i, 3 + 2i$<br>$-3$<br>$3 - 2i, -5 + 2i, 5 - 4i$<br>$1 + 4i, 1 - 4i$                        |
| $+3 + 10i$ | 1<br>2<br>3      | $1 + i, -1 - 2i, 1 - 4i$<br>$-3, 3 + 2i, 1 + 4i, -5 - 2i$<br>$-1 + 2i, 3 - 2i$                                    |
| $-7 + 8i$  | 0<br>1<br>2<br>3 | $1 + i, -7$<br>$3 + 2i, 3 - 2i, 1 - 4i, -5 - 2i$<br>$-1 - 2i, 1 + 4i, -5 + 2i, -1 - 6i$<br>$-1 + 2i, -3, -1 + 6i$ |

| Модуль   | Характер | Числа                            |
|----------|----------|----------------------------------|
| —11      | 0        | —3                               |
|          | 1        | $1+i, 3-2i, 1+4i, -5+2i, 5+4i$   |
|          | 2        | $-1+2i, -1-2i$                   |
|          | 3        | $3+2i, 1-4i, -5-2i, 5-4i$        |
| —11 + 4i | 0        | $1+i, -1+2i, 3+2i, 5+4i$         |
|          | 1        | $-1-2i, -1+6i$                   |
|          | 2        | $-5+2i$                          |
|          | 3        | $-3, 3-2i, 1+4i, 1-4i, -5-2i$    |
| +7 + 10i | 0        | $1+4i, 1-4i, -1+6i, -1-6i$       |
|          | 1        | $-1+2i, 3+2i, -5+2i$             |
|          | 2        | $1+i, 3-2i$                      |
|          | 3        | $-1-2i, -3, -5-2i$               |
| +11 + 6i | 0        | $1+i, -1+2i, -3, 1+4i, 1-4i, -7$ |
|          | 1        | $-1-2i, 3+2i, 3-2i$              |
|          | 2        | $-5-2i, -1+6i, 5-4i$             |
|          | 3        | $-5+2i, 5+4i, 7-2i.$             |

Теперь мы хотим попытаться получить индуктивным путем общие критерии для модулей, по которым заданное простое число имеет один и тот же характер. Мы все время предполагаем, что модули являются первичными среди ассоциированных с ними чисел, т. е. имеют вид  $a + bi$ , где или  $a \equiv 1, b \equiv 0$  или  $a \equiv 3, b \equiv 2 \pmod{4}$ .

В отношении числа  $1 + i$ , с которого мы начнем, на индуктивный закон натолкнуться будет легче, если мы отделим модули первого типа (для которых  $a \equiv 1, b \equiv 0$ ) от модулей второго типа (для которых  $a \equiv 3, b \equiv 2$ ). При помощи таблицы предыдущего пункта мы находим, что

| характер | соответствует модулям первого типа      |
|----------|-----------------------------------------|
| 0        | $5 + 4i, -7 + 8i, -7 - 8i, -11 + 4i$    |
| 1        | $1 - 4i, -3 + 8i, -3 - 8i, 9 + 4i, -11$ |
| 2        | $5 - 4i, -7, -11 - 4i$                  |
| 3        | $-3, 1 + 4i, 5 + 8i, 5 - 8i, 9 - 4i$    |

Если внимательно рассмотреть эти шестнадцать примеров, то мы найдем, что каждый раз характер  $\equiv \frac{1}{4}(a - b - 1)(\text{mod } 4)$ .

Точно так же

| характер | соответствует модулям второго типа                    |
|----------|-------------------------------------------------------|
| 0        | $3 - 2i, -1 - 6i, 7 + 2i, -5 + 6i, -1 + 10i, 11 + 6i$ |
| 1        | $-5 + 2i, -1 + 6i, 7 - 2i, -1 - 10i, 3 + 10i$         |
| 2        | $-1 + 2i, -5 - 2i, 3 - 10i, 7 + 10i$                  |
| 3        | $-1 - 2i, 3 + 2i, -5 - 6i, 7 - 10i, 11 - 6i$          |

Во всех этих двадцати примерах мы при некоторой внимательности замечаем, что характер  $\equiv \frac{1}{4}(a - b - 5)(\text{mod } 4)$ .

Оба эти правила легко можно объединить в одно, имеющее силу для модулей обоих типов, если учесть, что число  $b^2/4$  для модулей первого типа  $\equiv 0$ , а для модулей второго типа  $\equiv 1 (\text{mod } 4)$ . Поэтому характер числа  $1 + i$  по отношению к каждому простому и первичному среди ассоциированных с ним чисел модулю будет  $\equiv \frac{1}{4}(a - b - 1 - b^2)(\text{mod } 4)$ .

Попутно мы хотим здесь заметить, что так как  $(b + 1)^2$  всегда имеет вид  $8n + 1$ , т. е. число  $(2b + b^2)/4$  всегда четно, то указанный характер всегда будет четным или нечетным в зависимости от того, четно или нечетно число  $(a + b - 1)/4$ , что согласуется с указанным в п. 58 правилом для квадратичного характера

Так как числа  $\frac{1}{4}(a-b-1)$ ,  $\frac{1}{4}(a-b+3)$  являются целыми, и одно из них четно, а другое нечетно, то их произведение четно, и потому выполняется сравнение  $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod{4}$ . Поэтому вместо данного выше выражения для биквадратичного характера может быть взято также и следующее:

$$\frac{1}{4}(a-b-1-b^2) - \frac{1}{8}(a-b-1)(a-b+3) = \frac{1}{8}(-a^2 + 2ab - 3b^2 + 1);$$

эта форма предпочтительнее потому, что при ней не нужно ограничиваться лишь первичными модулями, а нужно предполагать только, что  $a$  нечетно, а  $b$  четно; действительно, при этом предположении одно из чисел  $a+bi$  или  $a-bi$ , очевидно, будет первичным среди ассоциированных, а значение указанной формулы для обоих этих чисел будет одинаковым.

64

Исходя из последнего найденного в предыдущем пункте правила, мы видим, что

| для<br>числа | характер $\equiv$                   |
|--------------|-------------------------------------|
| $-1+i$       | $\frac{1}{8}(a^2 + 2ab - b^2 - 1)$  |
| $-1-i$       | $\frac{1}{8}(-a^2 + 2ab + b^2 + 1)$ |
| $+1-i$       | $\frac{1}{8}(a^2 + 2ab + 3b^2 - 1)$ |

Это тотчас же следует из того, что для числа  $i$  характер  $\equiv \frac{1}{4}(a^2 + b^2 - 1)$ , а для числа  $-1$  характер  $\equiv \frac{1}{2}(a^2 + b^2 - 1) \equiv \frac{1}{2}b^2$ , так как  $a^2-1$  всегда имеет вид  $8n$ . Очевидно, что хотя эти четыре правила и получены пока на основании индуктивных заключений, но связаны между собой они так, что если будет получено доказательство одного из них, то тем самым будут доказаны и остальные.



ные. Едва ли нужно напоминать, что и в этих правилах предполагается только, что число  $a$  нечетно, а число  $b$  четно.

Если желательно использовать формулы, применимые только к первичным модулям, то можно использовать следующую схему.

| Для<br>числа | характер $\equiv$               |
|--------------|---------------------------------|
| $-1 + i$     | $\frac{1}{4}(-a - b + 1 - b^2)$ |
| $-1 - i$     | $\frac{1}{4}(a - b - 1 + b^2)$  |
| $+1 - i$     | $\frac{1}{4}(-a - b + 1 + b^2)$ |

Наиболее простые формулы получаются, если, как мы это делали в начале нашего индуктивного рассмотрения, различать модули первого и второго типа. Именно, характер

| числа    | для модулей первого<br>типа сравним с | для модулей второго<br>типа сравним с |
|----------|---------------------------------------|---------------------------------------|
| $-1 + i$ | $\frac{1}{4}(-a - b + 1)$             | $\frac{1}{4}(-a - b - 3)$             |
| $-1 - i$ | $\frac{1}{4}(a - b - 1)$              | $\frac{1}{4}(a - b + 3)$              |
| $+1 - i$ | $\frac{1}{4}(-a - b + 1)$             | $\frac{1}{4}(-a - b + 5)$             |

Для числа  $-1 + 2i$ , к которому мы теперь переходим, мы тоже хотим делать различие между теми модулями  $a + bi$ , для которых  $a \equiv 1$ ,  $b \equiv 0$ , и теми, для которых  $a \equiv 3$ ,  $b \equiv 2$ . Таблица п. 62 показывает, что в отношении этого числа

| характер | соответствует модулям первого типа        |
|----------|-------------------------------------------|
| 0        | $-3 + 8i, +5 - 8i, +9 + 4i, -11 + 4i$     |
| 1        | $+1 + 4i, +5 - 4i, -7, -3 - 8i$           |
| 2        | $+1 - 4i, +5 + 8i, -7 - 8i, -11$          |
| 3        | $-3, +5 + 4i, +9 - 4i, -7 + 8i, -11 - 4i$ |

Если привести эти отдельные модули к абсолютно наименьшим вычетам по модулю  $-1 + 2i$ , то мы заметим, что все те модули, которым соответствует характер 0, сравнимы с 1; те, которым соответствует характер 1, сравнимы с  $i$ ; те, характером которых является 2, сравнимы с  $-1$ ; наконец, те, характером которых является 3, сравнимы с  $-i$ . Но характерами чисел 1,  $i$ ,  $-1$ ,  $-i$  для модуля  $-1 + 2i$  как раз и являются соответственно числа 0, 1, 2, 3; таким образом, во всех этих семнадцати примерах характер числа  $-1 + 2i$  по отношению к модулю  $a + bi$  первого типа совпадает с характером числа  $a + bi$  по отношению к модулю  $-1 + 2i$ .

Точно так же при помощи таблицы мы находим, что

| характер | соответствует модулям второго типа                        |
|----------|-----------------------------------------------------------|
| 0        | $+3 + 2i, -5 - 2i, -1 + 10i, -1 - 10i, +11 + 6i$          |
| 1        | $+3 - 2i, -1 + 6i, -5 - 6i, +7 + 10i, +7 - 10i$           |
| 2        | $-5 + 2i, -1 + 6i, +7 - 2i$                               |
| 3        | $-1 - 2i, +7 + 2i, -5 + 6i, +3 + 10i, +3 - 10i, +11 - 6i$ |

Если привести эти модули к их абсолютно наименьшим вычетам по модулю  $-1 + 2i$ , то мы увидим, что все модули, которым соответствуют характеры 0, 1, 2, 3, сравнимы соответственно с числами  $-1$ ,  $-i$ ,  $+1$ ,  $+i$ ; но если, наоборот, взять за модуль число  $-1 + 2i$ , то сами эти числа будут соответственно иметь характеры 2, 3, 0, 1. Таким образом, во всех этих девятнадцати примерах характер числа  $-1 + 2i$  по отношению к модулю второго типа отличается от характера самого этого модуля по отношению к числу  $-1 + 2i$  на две единицы.

Далее, легко видеть, что совершенно так же обстоит дело и для числа  $-1 - 2i$ .

## 66

Для числа  $-3$  мы не будем делать различия между модулями первого и второго типа, ибо результат показывает, что такое различие здесь ни к чему. Итак,

| характер | соответствует модулям                                                                    |
|----------|------------------------------------------------------------------------------------------|
| 0        | $-1 + 6i, -1 - 6i, -7, -5 + 6i, -5 - 6i, -11, 11 + 6i, 11 - 6i$                          |
| 1        | $-1 - 2i, 1 - 4i, -5 + 2i, 5 + 4i, 7 + 2i, 5 - 8i, -1 + 10i, -7 - 8i, -11 - 4i, 7 - 10i$ |
| 2        | $3 + 2i, 3 - 2i, -3 + 8i, -3 - 8i, 9 + 4i, 3 + 10i, 3 - 10i$                             |
| 3        | $-1 + 2i, 1 + 4i, -5 - 2i, 5 - 4i, 7 - 2i, 5 + 8i, -1 - 10i, -7 + 8i, -11 + 4i, 7 + 10i$ |

Приведя эти модули к их наименьшим вычетам по модулю 3, мы увидим, что те, которым соответствует характер 0, либо  $\equiv 1$ , либо  $\equiv -1$ , те, характером которых является число 1, либо  $\equiv 1 - i$ , либо  $\equiv -1 + i$ , те, характером которых является число 2, либо  $\equiv i$ , либо  $\equiv -i$ , наконец, те, которые имеют характер 3, либо  $\equiv 1 + i$ , либо  $\equiv -1 - i$ . Отсюда мы индуктивным путем заключаем, что характер числа  $-3$  по отношению к простому и первичному среди ассоциированных чисел модулю совпадает с характером самого этого модуля, если за модуль уже брать число 3, или, что то же самое, число  $-3$ .

## 67

Проведя такое же индуктивное рассмотрение по отношению к другим простым числам, мы найдем, что для чисел  $3 \pm 2i, -1 \pm 6i, 7 \pm 2i, -5 \pm 6i, \dots$  справедливы теоремы, подобные той, к которой мы пришли в п. 65 для числа  $-1 + 2i$ , и, напротив, для чисел  $1 \pm 4i, 5 \pm 4i, -3 \pm 8i, 5 \pm 8i, 9 \pm 4i, \dots$  дело обстоит так же, как для числа  $-3$ . Таким образом, индукция приводит к следующей,

очень изящной теореме, которую мы по аналогии с теорией квадратичных вычетов в арифметике вещественных чисел можем назвать **фундаментальной теоремой теории биквадратичных вычетов**.

Если  $a + bi$ ,  $a' + b'i$  обозначают два различных и среди ассоциированных с ними чисел первичных, т. е. сравнимых по модулю  $2 + 2i$  с единицей, простых числа, то биквадратичный характер числа  $a + bi$  по отношению к модулю  $a' + b'i$  совпадает с характером числа  $a' + b'i$  по отношению к модулю  $a + bi$ , если или каждое, или по крайней мере одно из чисел  $a + bi$ ,  $a' + b'i$  принадлежит к первому типу, т. е. сравнимо по модулю 4 с единицей; напротив, оба эти характера отличаются один от другого на две единицы, если ни одно из чисел  $a + bi$ ,  $a' + b'i$  не принадлежит к первому типу, т. е. оба сравнимы по модулю 4 с числом  $3 + 2i$ .

Несмотря на большую простоту формулировки этой теоремы, доказательство ее принадлежит к наиболее глубоко скрытым тайнам высшей арифметики, так что, по крайней мере в настоящее время, оно может быть проведено только при помощи тончайших исследований, которые далеко вышли бы за рамки этого сочинения. Поэтому опубликование этого доказательства, так же, как и изложение связи этой теоремы с теми теоремами, с индуктивного установления которых мы начали это сочинение, мы отложим до третьего сочинения. Однако в заключение мы хотим все же привести уже здесь все, что необходимо для доказательства теорем, высказанных в пп. 63 и 64.

## 68

Мы начнем с тех простых чисел  $a + bi$ , для которых  $b = 0$  (т. е. с простых чисел третьего типа по терминологии п. 34) и для которых тем самым  $a$  должно быть (чтобы число было первичным среди ассоциированных) вещественным отрицательным простым числом вида  $-(4n + 3)$ , вместо которого мы будем писать  $-q$ . К такому виду принадлежат числа  $-3$ ,  $-7$ ,  $-11$ ,  $-19$ ...

Если обозначить через  $\lambda$  характер числа  $1 + i$ , когда за модуль берется одно из указанных чисел, то должно выполняться сравнение

$$i^\lambda \equiv (1 + i)^{(q^2-1)/4} \equiv 2^{(q^2-1)/8} i^{(q^2-1)/8} \pmod{q}.$$

Но известно, что число 2 является квадратичным вычетом или невычетом по модулю  $q$  в зависимости от того, имеет ли  $q$  вид  $8n + 7$  или  $8n + 3$ , откуда следует, что вообще

$$2^{(q-1)/2} \equiv (-1)^{(q+1)/4} \equiv i^{(q+1)/2} \pmod{q},$$

и потому, если возвести это соотношение в степень с показателем  $\frac{1}{4}(q+1)$ ,

$$2^{\frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{8}(q+1)^2} \pmod{q}.$$

Поэтому предыдущее соотношение принимает вид

$$i^\lambda \equiv i^{\frac{1}{8}(q+1)^2 + \frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{4}(q^2+q)} \pmod{q},$$

и отсюда следует, что

$$\lambda \equiv \frac{1}{4}(q^2+q) \equiv \frac{1}{4}(q+1)^2 - \frac{1}{4}(q+1) \pmod{4},$$

или, так как  $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$ , что

$$\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(q-1) \pmod{4}.$$

Это и представляет собой теорему п. 63 для случая  $b = 0$ .

## 69

Намного, однако, труднее исследовать такие модули  $a + bi$ , для которых  $b$  не равно нулю (числа четвертого типа по терминологии п.34), и здесь предварительно должны быть предпосланы различные исследования. Норму  $a^2 + b^2$ , которая является вещественным простым числом вида  $4n + 1$ , мы будем обозначать через  $p$ .

Обозначим через  $S$  совокупность всех наименьших вычетов по модулю  $a + bi = m$ , за исключением нуля, так что количество содержащихся в  $S$  чисел равно  $p - 1$ . Обозначим далее через  $x + yi$  произвольное число этой системы и положим  $ax + by = \xi$ ,  $ay - bx = \eta$ . Числа  $\xi$  и  $\eta$  являются поэтому целыми, заключенными между границами 0 и  $p$  (причем сами эти границы исключаются); в самом деле, в рассматриваемом случае, когда  $a$  и  $b$  взаимно просты, формулы п. 45, именно,  $\eta = k\xi$ ,  $\xi \equiv -k\eta \pmod{p}$  показывают, что ни одно

из чисел  $\xi$ ,  $\eta$  не может быть равно 0 без того, чтобы одновременно не исчезало бы и второе, т. е. чтобы не получалась бы комбинация  $x = 0$ ,  $y = 0$ , которую мы уже исключили. Таким образом, критерий того, что число  $x + yi$  содержится в  $S$ , состоит в том, что четыре числа  $\xi$ ,  $\eta$ ,  $p - \xi$ ,  $p - \eta$  должны быть положительными.

Далее, заметим, что ни для какого такого числа не может иметь место  $\xi = \eta$ , так как из этого следовало бы, что  $p(x + y) = a(\xi + \eta) + b(\xi - \eta) = 2a\xi$ , а это невозможно, так как ни один из сомножителей  $2$ ,  $a$ ,  $\xi$  не делится на  $p$ . Подобным же образом равенство  $p(x - y + a + b) = 2a\xi + (a + b)(p - \xi - \eta)$  показывает, что  $\xi + \eta$  не может быть равно  $p$ . Поэтому мы получаем отсюда, поскольку числа  $\xi - \eta$ ,  $p - \xi - \eta$  должны быть как положительными, так и отрицательными, разбиение системы  $S$  на четыре совокупности  $C$ ,  $C'$ ,  $C''$ ,  $C'''$ , причем мы полагаем содержащимися

| в сово-<br>купности | числа, для которых                                       |
|---------------------|----------------------------------------------------------|
| $C$                 | $\xi - \eta$ положительно, $p - \xi - \eta$ положительно |
| $C'$                | $\xi - \eta$ положительно, $p - \xi - \eta$ отрицательно |
| $C''$               | $\xi - \eta$ отрицательно, $p - \xi - \eta$ отрицательно |
| $C'''$              | $\xi - \eta$ отрицательно, $p - \xi - \eta$ положительно |

Таким образом, числа совокупности  $C$  характеризуются первоначально шестью условиями; именно, должны быть положительными шесть чисел  $\xi$ ,  $\eta$ ,  $p - \xi$ ,  $p - \eta$ ,  $\xi - \eta$ ,  $p - \xi - \eta$ ; но очевидно, что второе, пятое и шестое условия уже содержат в себе все остальные. Аналогично обстоит дело для совокупностей  $C'$ ,  $C''$ ,  $C'''$ , так что на самом деле полные критерии зависят от трех условий, а именно,

| для сово-<br>купности | должны быть положительны числа               |
|-----------------------|----------------------------------------------|
| $C$                   | $\eta$ , $\xi - \eta$ , $p - \xi - \eta$     |
| $C'$                  | $p - \xi$ , $\xi - \eta$ , $\xi + \eta - p$  |
| $C''$                 | $p - \eta$ , $\eta - \xi$ , $\xi + \eta - p$ |
| $C'''$                | $\xi$ , $\eta - \xi$ , $p - \xi - \eta$      |

Далее, каждый, даже если бы мы и не указывали на это, должен был заметить, что при геометрическом изображении комплексных чисел (ср. п. 39) числа системы  $S$  содержатся внутри квадрата, стороны которого пересекаются в точках, которыми изображаются числа  $0$ ,  $a + bi$ ,  $(1 + i)(a + bi)$ ,  $i(a + bi)$ , и что разбиение системы  $S$  соответствует разбиению квадрата его диагоналями. Однако нам хотелось бы использовать здесь чисто арифметические средства, почему мы и предоставляем ради краткости наглядные иллюстрации опытному читателю.

## 70

Если четыре комплексных числа

$$r = x + yi, \quad r' = x' + y'i, \quad r'' = x'' + y''i, \quad r''' = x''' + y'''i$$

так связаны между собой, что выполняются равенства

$$r' = m + ir, \quad r'' = m + ir' = (1 + i)m - r, \quad r''' = m + ir'' = im - ir,$$

и если предположить, что первое число,  $r$ , принадлежит совокупности  $C$ , то остальные числа,  $r'$ ,  $r''$ ,  $r'''$ , будут принадлежать соответственно совокупностям  $C'$ ,  $C''$ ,  $C'''$ .

Действительно, если положить

$$\begin{aligned} \xi &= ax + by, & \eta &= ay - bx, \\ \xi' &= ax' + by', & \eta' &= ay' - bx', \\ \xi'' &= ax'' + by'', & \eta'' &= ay'' - bx'', \\ \xi''' &= ax''' + by''', & \eta''' &= ay''' - bx''', \end{aligned}$$

то мы получим

$$\begin{aligned} \eta &= p - \xi' = p - \eta'' = \xi''', \\ \xi - \eta &= \xi' + \eta' - p = \eta'' - \xi'' = p - \xi''' - \eta''', \\ p - \xi - \eta &= \xi' - \eta' = \xi'' + \eta'' - p = \eta''' - \xi''', \end{aligned}$$

откуда при помощи критериев для отдельных совокупностей справедливость утверждения теоремы получается сама собой. И так как снова  $r = m + ir'''$ , то легко видеть, что если предположить число  $r$  принадлежащим совокупности  $C'$ , то числа  $r'$ ,  $r''$ ,  $r'''$  будут принадлежать соответственно совокупностям  $C''$ ,  $C'''$ ,  $C$ ; если предполо-

жить  $r$  принадлежащим совокупности  $C''$ , то остальные числа будут принадлежать совокупностям  $C'''$ ,  $C$ ,  $C'$ ; наконец, если  $r$  принадлежит совокупности  $C'''$ , то числа  $r'$ ,  $r''$ ,  $r'''$  принадлежат совокупностям  $C$ ,  $C'$ ,  $C''$ .

Одновременно из этого вытекает, что в отдельных совокупностях  $C$ ,  $C'$ ,  $C''$ ,  $C'''$  содержится по одинаковому количеству чисел, а именно, по  $(p-1)/4$  чисел.

## 71

**Теорема.** Если, понимая под  $k$  целое не делящееся на  $m$  число, умножить отдельные числа совокупности  $C$  на  $k$ , и после того как наименьшие вычеты этих произведений по модулю  $m$  распределены по совокупностям  $C$ ,  $C'$ ,  $C''$ ,  $C'''$ , обозначить количества тех, которые окажутся в этих отдельных совокупностях, соответственно через  $s$ ,  $s'$ ,  $s''$ ,  $s'''$ , то характер числа  $k$  по отношению к модулю  $m$  будет сравним по модулю 4 с числом  $s' + 2s'' + 3s'''$ .

**Доказательство.** Пусть к  $C$  принадлежит  $s$  наименьших вычетов  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta, \dots$ , к  $C'$  принадлежит  $s'$  вычетов  $m + i\alpha'$ ,  $m + i\beta'$ ,  $m + i\gamma'$ ,  $m + i\delta'$ ,  $\dots$ ; к  $C''$  принадлежит  $s''$  вычетов  $(1+i)m - \alpha''$ ,  $(1+i)m - \beta''$ ,  $(1+i)m - \gamma''$ ,  $(1+i)m - \delta''$ ,  $\dots$ ; наконец, к  $C'''$  принадлежит  $s'''$  вычетов  $im - i\alpha'''$ ,  $im - i\beta'''$ ,  $im - i\gamma'''$ ,  $im - i\delta'''$ ,  $\dots$ . Рассмотрим тогда четыре следующих произведения:

- 1) произведение всех  $(p-1)/4$  чисел, образующих совокупность  $C$ ;
- 2) произведение произведений, которые получаются при умножении этих отдельных чисел на  $k$ ;
- 3) произведение наименьших вычетов этих произведений, т. е. произведений чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta, \dots$ ,  $m + i\alpha'$ ,  $m + i\beta'$ ,  $\dots$ ;
- 4) произведение всех чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\delta, \dots$ ,  $\alpha'$ ,  $\beta'$ ,  $\gamma'$ ,  $\delta'$ ,  $\dots$ ,  $\alpha''$ ,  $\beta''$ ,  $\gamma''$ ,  $\delta''$ ,  $\dots$ , количество которых равно  $s + s' + s'' + s'''$ .

Если эти четыре произведения обозначить по порядку через  $P$ ,  $P'$ ,  $P''$ ,  $P'''$ , то мы, очевидно, будем иметь

$$P' \equiv k^{(p-1)/4} P, \quad P' \equiv P'', \quad P'' \equiv P''' i^{s'+2s''+3s'''} \pmod{m},$$

и потому

$$Pk^{(p-1)/4} \equiv P''' i^{s'+2s''+3s'''} \pmod{m}.$$



Но легко видеть, что все числа  $\alpha', \beta', \gamma', \delta', \dots, \alpha'', \beta'', \gamma'', \delta'', \dots, \alpha''', \beta''', \gamma''', \delta''', \dots$  принадлежат совокупности  $C$  и отличны как одно от другого, так и от чисел  $\alpha, \beta, \gamma, \delta, \dots$ , причем эти последние также различны между собой. Поэтому все эти числа вместе взятые совпадают, с точностью до порядка следования, со всеми числами, образующими совокупность  $C$ , откуда следует, что  $P = P'''$ , и потому

$$Pk^{(p-1)/4} \equiv P i^{c'+2c''+3c'''} \pmod{m}.$$

Наконец, отсюда получается, так как отдельные сомножители произведения  $P$  не делятся на  $m$ , что

$$k^{(p-1)/4} \equiv i^{c'+2c''+3c'''} \pmod{m},$$

так что число  $c' + 2c'' + 3c'''$  является характером числа  $k$  по отношению к модулю  $m$ .

## 72

Для того чтобы иметь возможность применить общую теорему предыдущего пункта к числу  $1 + i$ , мы должны совокупность  $C$  снова разбить на две меньшие совокупности  $G$  и  $G'$ , причем к совокупности  $G$  мы будем причислять те числа  $x + yi$ , для которых  $ax + by = \xi$  меньше чем  $p/2$ , а к совокупности  $G'$  — те, для которых  $\xi$  больше чем  $p/2$ ; количества чисел, содержащихся в совокупностях  $G$  и  $G'$ , мы обозначим через  $g$  и  $g'$ , так что  $g + g' = \frac{1}{4}(p-1)$ .

Таким образом, полным критерием принадлежности числа совокупности  $G$  является то, что положительны три числа  $\eta, \xi - \eta, p - 2\xi$ ; действительно, третье условие для совокупности  $C$ , согласно которому должно быть положительно число  $p - \xi - \eta$ , уже включается в этот критерий, так как  $p - \xi - \eta = (\xi - \eta) + (p - 2\xi)$ . Точно так же полный критерий для принадлежности числа совокупности  $G'$  состоит в положительности трех чисел  $\eta, p - \xi - \eta, 2\xi - p$ .

Отсюда легко видеть, что произведение каждого числа совокупности  $G$  на число  $1 + i$  принадлежит совокупности  $C'''$ . Действи-

тельно, если положить

$$(x + yi)(1 + i) = x' + y'i \text{ и } ax' + by' = \xi', \quad ay' - bx' = \eta',$$

то мы получим

$$\xi' = \xi - \eta, \quad \eta' - \xi' = 2\eta, \quad p - \xi' - \eta' = p - 2\xi,$$

т. е. критерий для принадлежности числа  $x + yi$  совокупности  $G$  совпадает с критерием для принадлежности числа  $x' + y'i$  совокупности  $C'''$ .

Совершенно аналогичным образом показывается, что произведение любого числа совокупности  $G'$  на число  $1 + i$  принадлежит совокупности  $C''$ .

Поэтому, если числу  $k$  из предыдущего пункта придать значение  $1 + i$ , то получится  $c = 0$ ,  $c' = 0$ ,  $c'' = g'$ ,  $c''' = g$ , и потому характер числа  $1 + i$  будет равен  $3g + 2g' = \frac{1}{2}(p - 1) + g$ . А так как характеры чисел  $i$ ,  $-1$  равны соответственно  $\frac{1}{4}(p - 1)$ ,  $\frac{1}{2}(p - 1)$ , то характерами чисел  $-1 + i$ ,  $-1 - i$ ,  $1 - i$  будут соответственно числа  $\frac{3}{4}(p - 1) + g$ ,  $g$ ,  $\frac{1}{4}(p - 1) + g$ . Тем самым вопрос сводится к определению числа  $g$ .

### 73

Рассуждения пп. 69 — 72 на самом деле не зависели от предположения, что  $m$  является первичным числом; начиная же с этого места, мы будем во всяком случае предполагать, что  $a$  нечетно, а  $b$  четно, и что, кроме того, числа  $a$ ,  $b$ ,  $a - b$  положительны. Прежде всего мы должны установить границы значений  $x$  для чисел совокупности  $G$ .

Если положить

$$ay - bx = \eta, \quad (a + b)x - (a - b)y = \zeta, \quad p - 2ax - 2by = \theta,$$

то критерий принадлежности числа  $x + yi$  к совокупности  $G$  будет состоять в трех условиях, а именно, в том, что числа  $\eta$ ,  $\zeta$ ,  $\theta$  должны

быть положительны. Так как  $px = (a - b)\eta + a\zeta$ ,  $p(a - 2x) = a\theta + 2b\eta$ , то должны быть положительны числа  $x$  и  $2a - x$ , т. е.  $x$  должно быть равно одному из чисел  $1, 2, 3, \dots, \frac{1}{2}(a - 1)$ . Так как, далее,  $(a - b)\theta = 2b\zeta + p(a - b - 2x)$ , то ясно, что если  $x$  меньше чем  $\frac{1}{2}(a - b)$ , то второе условие (согласно которому должно быть положительно  $\zeta$ ) уже содержит в себе третье (по которому должно быть положительно  $\theta$ ), и что, напротив, если  $x$  больше чем  $\frac{1}{2}(a - b)$ , то второе условие уже содержится в третьем. Поэтому для следующих значений числа  $x$ :  $1, 2, 3, \dots, \frac{1}{2}(a - b - 1)$  нужно позаботиться только о том, чтобы были положительны  $\eta$  и  $\zeta$ , т. е. чтобы  $y$  было больше чем  $bx/a$  и меньше чем  $(a + b)x/(a - b)$ . Следовательно, для каждого такого значения  $x$  всего имеется

$$\left[ \frac{(a + b)x}{a - b} \right] - \left[ \frac{bx}{a} \right]$$

чисел  $x + yi$ , если квадратные скобки имеют тот же смысл, в котором мы их уже употребляли в других случаях (ср. «Новое доказательство одной арифметической теоремы», п. 4; «Новые доказательства и обобщения фундаментальной теоремы теории квадратичных вычетов», «Новый алгоритм и т. д.», п. 3). Напротив, для следующих значений числа  $x$ :  $\frac{1}{2}(a - b + 1), \frac{1}{2}(a - b + 3), \dots, \frac{1}{2}(a - 1)$  достаточно, чтобы  $\eta$  и  $\theta$  принимали положительные значения, т. е. чтобы  $y$  было больше, чем  $bx/a$  и меньше чем  $(p - 2ax)/2b$ , или, что то же самое, чем  $\frac{1}{2}b + \frac{a^2 - 2ax}{2b}$ . Следовательно, для каждого такого значения всего имеется

$$\left[ \frac{1}{2}b + \frac{a^2 - 2ax}{2b} \right] - \left[ \frac{bx}{a} \right]$$

чисел  $x + yi$ .

Отсюда мы заключаем, что количество чисел в совокупности  $G$  равно

$$g = \sum \left[ \frac{(a + b)x}{a - b} \right] + \sum \left[ \frac{1}{2}b + \frac{a^2 - 2ax}{2b} \right] - \sum \left[ \frac{bx}{a} \right],$$

где в первом члене суммирование производится по всем целым значениям числа  $x$  от 1 до  $\frac{1}{2}(a-b-1)$ , во втором от  $\frac{1}{2}(a-b+1)$  до  $\frac{1}{2}(a-1)$  и в третьем — от 1 до  $\frac{1}{2}(a-1)$ .

Если мы используем букву  $\varphi$  в том же смысле, что и в указанном выше месте (ср. «*Новые доказательства и обобщения и т. д.*»), а именно, положим

$$\varphi(t, u) = \left[ \frac{u}{t} \right] + \left[ \frac{2u}{t} \right] + \left[ \frac{3u}{t} \right] + \dots + \left[ \frac{t'u}{t} \right],$$

где  $t, u$  обозначают какие-нибудь два положительных числа, а  $t'$  обозначает число  $\left[ \frac{1}{2}t \right]$ , то первый из указанных трех членов будет равен  $\varphi(a-b, a+b)$ , третий равен  $-\varphi(a, b)$ , а второй равен

$$\frac{1}{4}b^2 + \sum \left[ \frac{a^2 - 2ax}{2b} \right].$$

Но если мы напомним члены в обратном порядке, то получим

$$\sum \left[ \frac{a^2 - 2ax}{2b} \right] = \left[ \frac{a}{2b} \right] + \left[ \frac{3a}{2b} \right] + \left[ \frac{5a}{2b} \right] + \dots + \left[ \frac{(b-1)a}{2b} \right] = \varphi(2b, a) - \varphi(b, a).$$

Поэтому наша формула принимает вид

$$g = \varphi(a-b, a+b) + \varphi(2b, a) - \varphi(a, b) - \varphi(b, a) + \frac{1}{4}b^2.$$

Рассмотрим сначала член  $\varphi(a-b, a+b)$ , который тотчас же преобразуется в  $\varphi(a-b, 2b) + 1 + 2 + 3 + \dots + \frac{1}{2}(a-b-1)$  или в

$$\varphi(a-b, 2b) + \frac{1}{8}((a-b)^2 - 1).$$

Далее, так как, в силу общей теоремы,  $\varphi(t, u) + \varphi(u, t) = \left[ \frac{1}{2}t \right] \left[ \frac{1}{2}u \right]$ , если только  $t$  и  $u$  являются взаимно простыми положительными целыми числами, то

$$\varphi(a-b, 2b) = \frac{1}{2}b(a-b-1) - \varphi(2b, a-b),$$

и потому

$$\varphi(a-b, a+b) = \frac{1}{8}(a^2 + 2ab - 3b^2 - 4b - 1) - \varphi(2b, a-b).$$

Если члены выражения  $\varphi(2b, a - b)$  мы расположим следующим образом:

$$\left[ \frac{a-b}{2b} \right] + \left[ \frac{3(a-b)}{2b} \right] + \left[ \frac{5(a-b)}{2b} \right] + \dots + \left[ \frac{(b-1)(a-b)}{2b} \right] +$$

$$+ \left[ \frac{a-b}{b} \right] + \left[ \frac{2(a-b)}{b} \right] + \left[ \frac{3(a-b)}{b} \right] + \dots + \left[ \frac{\frac{1}{2}b(a-b)}{b} \right],$$

то второй ряд, очевидно, будет равен

$$\varphi(b, a - b) = \varphi(b, a) - 1 - 2 - 3 - \dots - \frac{1}{2}b = \varphi(b, a) - \frac{1}{8}(b^2 + 2b);$$

первый же ряд после изменения порядка расположения на обратный мы представим так:

$$\left[ \frac{1}{2}(a+1-b) - \frac{a}{2b} \right] + \left[ \frac{1}{2}(a+3-b) - \frac{3a}{2b} \right] +$$

$$+ \left[ \frac{1}{2}(a+5-b) - \frac{5a}{2b} \right] + \dots + \left[ \frac{1}{2}(a-1) - \frac{(b-1)a}{2b} \right],$$

а так как, если  $t$  обозначает целое, а  $u$  — дробное число, всегда будет  $[t - u] = t - 1 - [u]$ , то это выражение преобразуется к следующему:

$$\frac{1}{8}b(2a - 4 - b) - \left[ \frac{a}{2b} \right] - \left[ \frac{3a}{2b} \right] - \left[ \frac{5a}{2b} \right] - \dots - \left[ \frac{(b-1)a}{2b} \right] =$$

$$= \frac{1}{8}b(2a - 4 - b) - \varphi(2b, a) + \varphi(b, a).$$

Поэтому

$$\varphi(2b, a - b) = 2\varphi(b, a) - \varphi(2b, a) + \frac{1}{4}b(a - 3 - b),$$

а, значит,

$$\varphi(a - b, a + b) = \varphi(2b, a) - 2\varphi(b, a) + \frac{1}{8}(a^2 - b^2 + 2b - 1).$$

Если подставить это значение в приведенную выше формулу для  $g$  и положить, кроме того,  $\varphi(a, b) + \varphi(b, a) = \frac{1}{4}b(a - 1)$ , то мы получим

$$g = 2\varphi(2b, a) - 2\varphi(b, a) + \frac{1}{8}(a^2 - 2ab + b^2 + 4b - 1).$$

При помощи совершенно аналогичных рассуждений исследуется случай, когда, хотя  $a$ ,  $b$  и остаются положительными, но  $a - b$  отрицательно, т. е.  $b - a$  положительно. Равенства  $p(a - 2x) = 2b\eta + a\theta$ ,  $p(b - a + 2x) = 2b\zeta + (b - a)\theta$  показывают, что числа  $\frac{1}{2}a - x$  и  $x + \frac{1}{2}(b - a)$  должны быть положительны, и потому  $x$  должно быть равно одному из чисел  $-\frac{1}{2}(b - a - 1)$ ,  $-\frac{1}{2}(b - a - 3)$ ,  $-\frac{1}{2}(b - a - 5), \dots, +\frac{1}{2}(a - 1)$ . Далее, из равенства  $px + (b - a)\eta = a\zeta$  следует, что для отрицательных значений  $x$  условие, согласно которому должно быть положительно  $\eta$ , уже содержится в условии, согласно которому должно быть положительно  $\zeta$ , и что, наоборот, если числу  $x$  придается положительное значение, то из положительности числа  $\zeta$  вытекает положительность числа  $\eta$ . Поэтому значения числа  $y$  для определенного отрицательного значения числа  $x$  должны содержаться между  $(a + b)x/(a - b)$  и  $(p - 2ax)/2b$ , а для заданного положительного значения числа  $x$  — между  $bx/a$  и  $(p - 2ax)/2b$ . Для  $x = 0$  эти границы, очевидно, равны 0 и  $p/2b$ , исключая само значение  $y = 0$ . Из этого следует, что

$$g = - \sum \left[ \frac{(a + b)x}{a - b} \right] + \sum \left[ \frac{1}{2}b + \frac{a^2 - 2ax}{2b} \right] - \sum \left[ \frac{bx}{a} \right],$$

где в первом члене суммирование производится по всем отрицательным значениям  $x$  от  $-1$  до  $-\frac{1}{2}(b - a - 1)$ , во втором — по всем значениям  $x$  от  $-\frac{1}{2}(b - a - 1)$  до  $\frac{1}{2}(a - 1)$ , и в третьем — по всем положительным значениям  $x$  от  $+1$  до  $\frac{1}{2}(a - 1)$ . Таким образом, в результате первого суммирования получается  $-\varphi(b - a, b + a)$ , в результате второго, так же, как и в предыдущем пункте, получается  $\frac{1}{4}b^2 + \varphi(2b, a) - \varphi(b, a)$ , и, наконец, в результате третьего суммирования получается  $-\varphi(a, b)$ , т. е.

$$g = -\varphi(b - a, b + a) + \varphi(2b, a) - \varphi(b, a) - \varphi(a, b) + \frac{1}{4}b^2.$$

Точно таким же образом, как в предыдущем пункте, мы получаем теперь

$$\begin{aligned}\varphi(b-a, b+a) &= \varphi(b-a, 2b) - \frac{1}{8}((b-a)^2 - 1) = \\ &= \frac{1}{8}(3b^2 - 2ab - a^2 - 4b + 1) - \varphi(2b, b-a),\end{aligned}$$

и

$$\varphi(2b, b-a) = \varphi(2b, a) - 2\varphi(b, a) + \frac{1}{4}b(b-1-a),$$

откуда

$$\varphi(b-a, b+a) = 2\varphi(b, a) - \varphi(2b, a) + \frac{1}{8}(b^2 - a^2 - 2b + 1),$$

и, наконец,

$$g = 2\varphi(2b, a) - 2\varphi(b, a) + \frac{1}{8}(a^2 - 2ab + b^2 + 4b - 1).$$

Таким образом, доказано, что  $g$  выражается одной и той же формулой, независимо от того, положительно число  $a-b$  или отрицательно, лишь бы были положительны числа  $a, b$ .

## 75

Чтобы получить дальнейшую редукцию, положим

$$L = \left[ \frac{a}{2b} \right] + \left[ \frac{2a}{2b} \right] + \left[ \frac{3a}{2b} \right] + \dots + \left[ \frac{\frac{1}{2}ba}{2b} \right],$$

$$M = \left[ \frac{\left(\frac{1}{2}b+1\right)a}{2b} \right] + \left[ \frac{\left(\frac{1}{2}b+2\right)a}{2b} \right] + \left[ \frac{\left(\frac{1}{2}b+3\right)a}{2b} \right] + \dots + \left[ \frac{ba}{2b} \right],$$

$$N = \left[ \frac{a+b}{2b} \right] + \left[ \frac{2a+b}{2b} \right] + \left[ \frac{3a+b}{2b} \right] + \dots + \left[ \frac{\frac{1}{2}ba+b}{2b} \right].$$

Так как легко видеть, что всегда  $[u] + \left[ u + \frac{1}{2} \right] = [2u]$ , какую бы вещественную величину  $u$  ни обозначало, то  $L + N = \varphi(b, a)$ ,

а так как очевидно, что  $L + M = \varphi(2b, a)$ , то

$$\varphi(2b, a) - \varphi(b, a) = M - N.$$

Далее, ясно, что для суммы первого члена ряда  $N$  и предпоследнего члена ряда  $M$  имеет место  $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right] = \frac{1}{2}(a-1)$ , и что такова же будет сумма второго члена ряда  $N$  и третьего с конца члена ряда  $M$  и т. д. А так как, кроме того, последний член ряда  $M$  равен  $\frac{1}{2}(a-1)$ , а последний член ряда  $N$  равен  $\left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$ , где нужно брать верхний или нижний знак в зависимости от того, имеет ли число  $a$  вид  $4n+1$  или  $4n+3$ , то выполняется равенство

$$M + N = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1),$$

и потому

$$\varphi(2b, a) - \varphi(b, a) = \frac{1}{4}(a-1)b + \frac{1}{4}(a \mp 1) - 2N.$$

Следовательно, формула для  $g$ , найденная в пп. 73 и 74, переходит в формулу

$$g = \frac{1}{8}((a+b)^2 - 1) + 2n - 4N,$$

если положить  $a \mp 1 = 4n$ , где  $n$  есть целое число. Но так как отсюда получается, что  $1 = 16n^2 - 8an + a^2$ , то эта формула может быть представлена также и следующим образом:

$$g = \frac{1}{8}(-a^2 + 2ab + b^2 + 1) + 4\left(\frac{1}{2}(a+1)n - n^2 - N\right).$$

Но так как  $g$  является характером числа  $-1-i$  по модулю  $a+bi$ , то этот характер, следовательно, будет  $\equiv \frac{1}{8}(-a^2 + 2ab + b^2 + 1) \pmod{4}$ , а это как раз и есть теорема, найденная выше (п. 64) индуктивным путем; отсюда немедленно получаются и теоремы относительно характеров чисел  $1+i$ ,  $1-i$ ,  $-1+i$ . Таким образом, для случая, когда  $a$  и  $b$  положительны, эти четыре теоремы доказаны теперь со всей строгостью.



Если  $b$  отрицательно, в то время как  $a$  остается положительным, то положим  $b = -b'$ , где  $b'$  уже положительно. Так как уже доказано, что по модулю  $a + b'i$  характер числа  $-1 - i$  сравним с  $\frac{1}{8}(-a^2 + 2ab' + b'^2 + 1)$  по модулю 4, то характер числа  $-1 + i$  по модулю  $a - b'i$ , согласно приведенной в п. 62 теореме, будет  $\equiv \frac{1}{8}(a^2 - 2ab' - b'^2 - 1)$ , т. е. характер числа  $-1 + i$  по модулю  $a + bi$  будет  $\equiv \frac{1}{8}(a^2 + 2ab - b^2 - 1)$ ; а это как раз и есть теорема, указанная в п. 64, из которой сразу получаются и остальные три теоремы, касающиеся характеров чисел  $1 + i$ ,  $1 - i$ ,  $-1 - i$ . Таким образом, эти теоремы доказаны также и для случая, когда  $b$  отрицательно, т. е. для всех случаев, когда  $a$  положительно.

Наконец, если  $a$  отрицательно, то положим  $a = -a'$ ,  $b = -b'$ . Но так как, в силу уже доказанного, характер числа  $1 + i$  относительно модуля  $a' + b'i$  будет  $\equiv \frac{1}{8}(-a'^2 + 2a'b' - 3b'^2 + 1) \pmod{4}$ , и так как безразлично, брать ли за модуль число  $a' + b'i$  или противоположное число  $-a' - b'i$ , то характер числа  $1 + i$  по отношению к модулю  $a + bi$  будет, очевидно,  $\equiv \frac{1}{8}(-a^2 + 2ab - 3b^2 + 1) \pmod{4}$ , и подобные же утверждения имеют силу для характеров чисел  $1 - i$ ,  $-1 + i$ ,  $-1 - i$ .

Таким образом, из этого следует, что доказательство теорем о характерах чисел  $1 + i$ ,  $1 - i$ ,  $-1 + i$ ,  $-1 - i$  (пп. 63 и 64) теперь уже свободно от всяких ограничительных предположений.

---

НЕКОТОРЫЕ  
ИССЛЕДОВАНИЯ  
ИЗ РУКОПИСНОГО  
НАСЛЕДИЯ  
ГАУССА





## УЧЕНИЕ О ВЫЧЕТАХ

### I

#### Решение сравнения $X^m - 1 \equiv 0$

237 \*

В третьем разделе мы показали, что сравнение  $x^n \equiv 1$ , когда за модуль берется простое число  $p$ , обладает  $\mu$  корнями, где  $\mu$  является наибольшим общим делителем  $n$  и  $p - 1$ , и что эти корни в точности совпадают с корнями сравнения  $x^\mu \equiv 1$ . Поэтому достаточно рассмотреть только тот случай, когда  $n$  является делителем числа  $p - 1$ . А то, что решение не только этого сравнения  $x^n \equiv 1$ , но и любого другого по любому модулю может быть выведено из решения по модулям, которые являются простыми числами, было уже показано раньше, а ниже (в восьмом разделе) будет изучено еще подробнее.

238

Но мы можем еще больше упростить нашу задачу; действительно, в том же разделе мы установили, что решение сравнения  $x^n \equiv 1$  зависит от решений подобных же сравнений  $x^a \equiv 1$ ,  $x^b \equiv 1, \dots$ , где числа  $a, b, \dots$  являются либо простыми, либо степенями простых, а  $n$  есть произведение этих чисел. Именно, если  $A, B, \dots$  являются соответственно некоторыми корнями сравнений  $x^a \equiv 1$ ,  $x^b \equiv 1, \dots$ ,

---

\* Номера отдельных пунктов оставлены те же, что и в рукописи Гаусса.—  
*Прим. перев.*

то их произведение  $AB \dots$  равно одному из корней сравнения  $x^n \equiv 1$ . Поэтому мы ограничим наше исследование решением сравнения  $x^n \equiv 1 \pmod{p}$ , где  $p$  является простым числом, а  $n$  равно простому числу или степени простого числа и одновременно является делителем числа  $p - 1$ .

## 239

Далее, из третьего раздела известно, что среди корней сравнения  $x^n \equiv 1$  всегда имеются такие, степенями которых могут быть представлены все остальные корни. Если  $r$  обозначает один из таких корней (мы называли их выше первообразными корнями, когда было  $n = p - 1$ , и это же выражение мы хотим и далее употреблять в расширенном смысле), то все корни заданного сравнения суть

$$1, r, r^2, r^3, \dots, r^{n-1}.$$

Таким образом, мы должны направить все наши усилия на то, чтобы получить такие корни, ибо, если они будут найдены, то остальные корни получатся сами собой. Для краткости мы будем обозначать некоторую степень числа  $r$  посредством ее показателя, заключенного в скобки, так что  $(0)$  будет обозначать единицу,  $(1)$  — некоторый первообразный корень сравнения  $x^n \equiv 1$ ,  $(2)$  — квадрат числа  $(1)$ , и т. д., так что ряд  $(0), (1), (2), (3), \dots, (n - 1)$  будет охватывать все корни. При этом известно, что  $(k)$  всегда будет первообразным корнем, когда  $k$  взаимно просто с  $n$ , т. е. в нашем случае (где  $n$  является степенью простого числа  $t$ , скажем,  $n = t^v$ ), когда  $t$  не входит делителем в  $k$ . Очевидно, что обозначения  $(1), (2), \dots$  сами по себе неопределенны, однако, если  $(1)$  получает некоторое определенное значение, то и все остальные выражения уже будут определены.

## 240

Так как мы поставили себе целью сначала искать первообразные корни, то мы должны прежде всего отделить их от остальных. Это достигается выбрасыванием из ряда  $(0), (1), (2), \dots, (n - 1)$

всех членов, в которых  $k$  делится на  $t$ ; если же  $n$  является простым числом, т. е.  $v = 0$ , то нужно отбросить только один член (0). Однако, прежде чем переходить к дальнейшему исследованию, мы очень советуем читателю рассмотреть несколько примеров, для того чтобы иметь конкретное представление обо всем, что без этого могло бы показаться слишком абстрактным. Хотя мы приводим здесь только один пример, читателю будет не лишне самому разобрать и другие примеры.

Если  $p = 29$ ,  $n = 7$ , то семью корнями сравнения  $x^7 \equiv 1 \pmod{29}$  являются: 1, 7, 16, 20, 23, 24, 25. Так как  $n$  является простым числом, то все эти корни, за исключением 1, являются первообразными; таким образом, если положить  $7 = (1)$ , то обозначения

$$(0), (1), (2), (3), (4), (5), (6)$$

будут соответственно иметь следующие значения:

$$1, 7, 20, 24, 23, 16, 25.$$

При этом учитывается, что значения  $(n)$  и  $(0)$ ,  $(n + 1)$  и  $(1)$  и т. д. и вообще  $(a)$  и  $(b)$  эквивалентны, если  $a \equiv b \pmod{n}$ .

## 241

Однако, чтобы достигнуть нашей цели, мы должны действовать еще несколько иным способом. Именно, мы сохраним только те члены  $(k)$ , у которых  $k$  не делится на  $t$ , и количество которых равно  $\frac{t-1}{t} \cdot n = \lambda$ ; а все эти числа (или числа, сравнимые с ними по модулю  $n$ ) могут быть представлены следующими одна за другой степенями какого-нибудь одного числа.

Если это число равно  $\rho$ , то все первообразные корни сравнения  $x^n \equiv 1$  будут обозначаться следующим образом:

$$(1), (\rho), (\rho^2), (\rho^3), \dots, (\rho^{\lambda-1}).$$

Этим приемом мы добиваемся того, что все непервообразные корни совершенно исключаются; основания для этого и получаемые преимущества ниже будут пояснены отчетливее. В нашем примере мы можем, таким образом, положить  $\rho = 3$ ; тогда первообразные

корни сравнения  $x^7 \equiv 1$  расположатся так:

|             |                                                                                       |
|-------------|---------------------------------------------------------------------------------------|
|             | (1), (3), (3 <sup>2</sup> ), (3 <sup>3</sup> ), (3 <sup>4</sup> ), (3 <sup>5</sup> ), |
| или         | (1), (3), (2), (6), (4), (5),                                                         |
| и они равны | 7. 24, 20, 25, 23, 16.                                                                |

## 242

Для того чтобы читатель знал, куда нацелены дальнейшие исследования, мы укажем теорему, которую мы хотим доказать и пояснить.

Если число  $\lambda$  (которое равно  $t^{v-1}(t-1)$ ) имеет простые сомножители  $a, b, c, d, \dots$ , и  $\lambda = a^\alpha b^\beta c^\gamma \dots$ , то решение сравнения  $x^n - 1 \equiv 0$  сводится к решению  $\alpha + \beta + \dots$  сравнений более низкой степени, из которых  $\alpha$  сравнений имеет степень  $a$ ,  $\beta$  сравнений — степень  $b$ ,  $\gamma$  сравнений — степень  $c$ , и т. д.

Так, в нашем примере решение сравнения  $x^7 \equiv 1$  зависит от одного сравнения второй степени и одного сравнения третьей степени, и вообще легко видеть, что степень этих сравнений никогда не зависит от модуля  $p$ . Однако, чтобы получить доказательство этой теоремы, мы должны предпослать некоторые теоремы, касающиеся связи между сравнениями и их корнями, хотя сами эти исследования будут продолжены только в восьмом разделе.

## 243

**Теорема.** Если сравнение

$$x^m + Ax^{m-1} + Bx^{m-2} + \dots + N \equiv 0 \text{ (по простому модулю)}$$

обладает тем свойством, что для произведения  $m$  сомножителей  $x - r, x - r', x - r'', x - r''', \dots$ , которое мы обозначим через  $x^m + ax^{m-1} + bx^{m-2} + \dots + n$ , имеет место  $A \equiv a, B \equiv b, C \equiv c, \dots$ , по модулю  $p$ , то величины  $r, r', r'', \dots$  будут корнями заданного сравнения, причем других корней оно иметь не будет.

**Доказательство.** I. Всегда

$$x^m + Ax^{m-1} + Bx^{m-2} + \dots \equiv x^m + ax^{m-1} + bx^{m-2} + \dots \pmod{p}.$$

II. Если бы заданному сравнению удовлетворяло еще какое-нибудь значение  $\rho$ , которое не сравнимо ни с одним из чисел  $r, r', r'', \dots$ , то выполнялось бы сравнение

Но так как ни один из сомножителей  $\rho - r, \rho - r', \rho - r'', \dots$  не сравним с 0, то и произведение их всех не может быть сравнимо с 0. Поэтому других корней, кроме  $r, r', \dots$ , нет. Это второе утверждение теоремы.

**Задача.** Пусть  $r, r', r'', \dots$  — неизвестные величины, число которых равно  $t$ , и пусть сумма их равна  $\alpha$ , сумма их квадратов равна  $\beta$ , сумма кубов равна  $\gamma$ , и т. д., и сумма  $t$ -х степеней равна  $\mu$ ; даны, однако, не сами эти числа (количество которых тоже равно  $t$ ), а другие числа,  $\alpha', \beta', \gamma', \dots$ , которые соответственно сравнимы с ними по модулю  $p$ , являющемуся простым числом, большим чем  $t$ . Нужно найти сравнение  $t$ -й степени, корнями которого являются  $r, r', r'', \dots$ .

и определим его коэффициенты  $A, B, C, \dots$  (используя вместо уравнения сравнение) при помощи известного метода, именно, полагая

$$\begin{aligned} -A &\equiv \alpha', \\ -2B &\equiv \beta' + A\alpha', \\ -3C &\equiv \gamma' + A\beta' + B\alpha', \\ -4D &\equiv \delta' + A\gamma' + B\beta' + C\alpha', \\ &\dots\dots\dots \\ -mN &\equiv \mu' + A\lambda' + \dots \end{aligned}$$



Эти коэффициенты не могут, однако, быть неопределенными, потому что все числа  $1, 2, 3, \dots, n < p$ . Тогда я утверждаю, что сравнение

$$x^m + Ax^{m-1} + Bx^{m-2} + \dots + N \equiv 0$$

является искомым.

**Доказательство.** Предположим, что уравнение, корнями которого являются  $r, r', r'', r''', \dots$ , следующее:

$$x^m + ax^{m-1} + bx^{m-2} + \dots = 0.$$

Тогда

$$\begin{aligned} -a &= \alpha, \\ -2b &= \beta + a\alpha, \\ -3c &= \gamma + a\beta + b\alpha, \\ -4d &= \delta + a\gamma + b\beta + c\alpha, \\ &\dots \end{aligned}$$

Но тогда, очевидно,

$$a \equiv A, \quad b \equiv B, \quad c \equiv C, \dots (\text{mod } p),$$

и потому, согласно предыдущему пункту, числа  $r, r', r'', \dots$ , которые являются корнями уравнения

$$x^m + ax^{m-1} + bx^{m-2} + \dots = 0,$$

будут одновременно и корнями сравнения

$$x^m + Ax^{m-1} + Bx^{m-2} + \dots \equiv 0.$$

Мы предоставляем читателю привести примеры.

Мы возвращаемся к нашей задаче. Сохраняя обозначения, использованные в п. 242 и предыдущем пункте, мы хотим показать, что если  $\lambda$  является произведением нескольких сомножителей  $efg\dots$ , то первообразные корни сравнения  $x^n \equiv 1$ , количество которых равно  $\lambda$ , могут быть так разбиты на  $e$  классов, что суммы корней, причисленных к одному и тому же классу, даются сравнением  $e$ -й степени; далее, что если классы считать известными, то каждый из них может быть в свою очередь так разбит на  $f$  порядков, что

сумма каждого порядка дается сравнением  $f$ -й степени, а эти порядки снова могут быть подразделены, и т. д., до тех пор, пока мы не придем к отдельным корням.

246

**Определение.** Совокупность *всех* содержащихся в форме  $(\rho^{ke+\alpha})$  (п. 241) членов мы будем называть **полным периодом** или просто **периодом**. Пусть  $e$  обозначает какой-нибудь делитель числа  $\lambda$ ,  $\alpha$ —какое-нибудь заданное число,  $k$ —всевозможные целые числа от 0 до  $\frac{\lambda}{e} - 1$ ; тогда ради краткости мы будем обозначать такой период через  $(e * \alpha)$ . Так, в нашем примере члены

$$\begin{array}{llll} (1), (2), (4) & \text{образуют период} & (2 * 0), \\ (3), (6), (5) & \text{»} & (2 * 1), \\ (1), (6) & \text{»} & (3 * 0), \\ (3), (4) & \text{»} & (3 * 1), \\ (2), (5) & \text{»} & (3 * 2). \end{array}$$

*Если теперь все члены некоторым образом разбиты на периоды, отдельные периоды снова разбиты на меньшие периоды и т. д., то мы утверждаем, что этим самым мы добиваемся того, что было высказано в предыдущем пункте.*

Однако, прежде чем приступить к изложению этого, мы покажем, что хотя при образовании такого периода используются в некотором смысле произвольные величины  $r, \rho$ , тем не менее не получается никакой неопределенности, т. е. что как бы эти величины не выбирались, в одном и том же периоде все время будут получаться одни и те же члены (именно, если предписано, сколько членов период должен содержать).

Критерий принадлежности двух членов  $A, B$  к одному и тому же периоду получается из того, что каждый из них имеет вид  $(\rho^{ke+\alpha})$ , т. е. что  $A \equiv r^{\rho^{ke+\alpha}}, B \equiv r^{\rho^{k'e+\alpha}} \pmod{p}$ . При этом  $r$  является первообразным корнем сравнения  $x^n \equiv 1 \pmod{p}$ , а  $\rho$ —первообразным корнем сравнения  $x^\lambda \equiv 1 \pmod{n}$  (ср. выше).

Нужно доказать, что если вместо чисел  $r, \rho$  выбраны другие числа, например,  $s, \sigma$ , то  $A$  и  $B$  будут содержаться в подобных формах  $s^{\sigma l e + \beta}, s^{\sigma l' e + \beta}$ .

Пусть  $s^m \equiv r \pmod{p}$ ,  $\sigma^\mu \equiv \rho \pmod{n}$  и  $m \equiv \sigma^\zeta \pmod{n}$ , что возможно, так как  $r, \rho$  являются первообразными корнями;  $m$  взаимно просто с  $n$ ,  $\mu$  взаимно просто с  $\lambda$  (раздел III). После соответствующей подстановки мы получаем  $A \equiv s^{\sigma \mu k e + \mu \alpha + \zeta}$ ,  $B \equiv s^{\sigma \mu k' e + \mu \alpha + \zeta}$ , что и требовалось доказать.

## 247

**Теорема.** Произведение двух однотипных периодов независимо от числа  $p$  может быть образовано сложением однотипных периодов и заданных чисел.

(Однотипными периодами мы называем такие периоды, которые содержат одинаковое количество членов, т. е. для которых число  $e$  одно и то же.)

**Пример.** Если  $n = 7$ , то произведение периодов  $(1) + (6)$  и  $(2) + (5)$  (в силу  $(a) \cdot (b) = (a + b)$ ) равно  $(3) + (6) + (8) + (11)$ , т. е. состоит из периодов  $(3) + (4)$  и  $(1) + (6)$ .

**Доказательство.** Пусть  $\frac{\lambda}{e} = f$  и заданные периоды суть  $(e * \alpha)$  и  $(e * \beta)$ , а суммы —

$$\begin{aligned} (\rho^\alpha) + (\rho^{\alpha+e}) + (\rho^{\alpha+2e}) + \dots + (\rho^{\alpha+(f-1)e}) &= P, \\ (\rho^\beta) + (\rho^{\beta+e}) + (\rho^{\beta+2e}) + \dots + (\rho^{\beta+(f-1)e}) &= Q. \end{aligned}$$

Произведение  $PQ$  будет состоять из  $f^2$  членов. Упорядочим их следующим образом. Образует  $f$  рядов, каждый из которых состоит из  $f$  членов. Первый ряд охватывает произведение  $P$  на  $(\rho^\beta)$ , второй — произведение  $P$  на  $(\rho^{\beta+e})$  и т. д. В первом ряду первое место занимает произведение, которое получается из члена  $(\rho^\alpha)$ , второе место — произведение, которое получается из  $(\rho^{\alpha+e})$ , и т. д. по порядку; во втором же ряду первое место будет принадлежать произведению, получающемуся из члена  $(\rho^{\alpha+e})$ , второе — произведению, получающемуся из члена  $(\rho^{\alpha+2e})$ , и т. д., наконец, последнее — произведению, получающемуся из члена  $(\rho^\alpha)$ ; третий ряд пусть начинается с произведения, получающегося из члена  $(\rho^{\alpha+2e})$ , и т. д., а

за произведением последнего члена пусть следуют произведения первого, второго и т. д. членов; иными словами, если следующие один за другим члены периода  $P$  обозначены через  $1, 2, 3, \dots, z$ , а следующие один за другим члены периода  $Q$  — через  $I, II, III, \dots, Z$ , то получаются следующие части произведения  $PQ$ :

$$\begin{aligned} &1 \cdot I + 2 \cdot I + 3 \cdot I + 4 \cdot I + \dots + z \cdot I, \\ &2 \cdot II + 3 \cdot II + 4 \cdot II + \dots + 1 \cdot II, \\ &3 \cdot III + 4 \cdot III + \dots + 1 \cdot III + 2 \cdot III, \\ &\dots \end{aligned}$$

Составим теперь из членов, которые занимают в отдельных рядах одинаковые места,  $f$  порядков. Тогда я утверждаю, что

1) если какой-нибудь член сравним с 1, то и все остальные члены того же порядка тоже сравнимы с 1;

2) каждый порядок, в котором нет членов, сравнимых с 1, образует период.

Если мы это докажем, то мы, очевидно, достигнем нашей цели.

Общий вид такого порядка таков:

$$\begin{aligned} &(\rho^{\alpha+ke} + \rho^{\beta}), \quad (\rho^{\alpha+(k+1)e} + \rho^{\beta+e}), \\ &(\rho^{\alpha+(k+2)e} + \rho^{\beta+2e}), \dots, (\rho^{\alpha+(k+f-1)e} + \rho^{\beta+(f-1)e}); \end{aligned}$$

действительно, вместо  $\rho^{\alpha+(k-1)e}$  можно написать также  $\rho^{\alpha+(k+f-1)e}$ , ибо  $ef = \lambda$  и  $\rho^{\lambda} \equiv 1 \pmod{n}$ , и так же обстоит дело в отношении предыдущих членов. Если положить  $\rho^{\alpha+ke} + \rho^{\beta} \equiv \rho^{\kappa} \pmod{n}$ , что допустимо, если  $\rho^{\alpha+ke} + \rho^{\beta}$  не делится на  $n$ , то порядок можно будет представить также и так:

$$(\rho^{\kappa}), (\rho^{\kappa+e}), (\rho^{\kappa+2e}), \dots, (\rho^{\kappa+(f-1)e}),$$

а это, очевидно, есть период  $(e * \kappa)$ ; если же  $\rho^{\alpha+ke} + \rho^{\beta}$  делится на  $n$ , то все члены порядка будут сравнимы с 1.

**З а м е ч а н и е.** Это доказательство одновременно дает очень простой прием для нахождения произведения; ниже мы дадим другой прием, который хотя и не предпочтительнее этого, но вследствие своей простоты также заслуживает большого внимания.

Все меньшие периоды, которые образуют один больший период, мы будем называть **системой периодов**. Так, например, это наименование будет употребляться для периодов

$$(ef * \alpha), (ef * f + \alpha), (ef * 2f + \alpha), \dots, (ef * (e - 1)f + \alpha),$$

из которых составлен период  $(f * \alpha)$ . Система периодов будет *правильно расположена*, если числа, стоящие после звездочки \*, как в данном случае числа  $\alpha, f + \alpha, 2f + \alpha, \dots$ , образуют арифметическую прогрессию (с разностью  $f$ ); наконец, системы будут *однотипными*, если как меньшие, так и большие периоды однотипны.

**Теорема.** *Если перемножить один с другим периоды двух правильно расположенных систем, а именно, первый перемножить с первым, второй со вторым, третий с третьим и т. д., то сумма всех произведений может быть составлена из периодов, однотипных с большим периодом, и заданных чисел.*

**Доказательство.** Пусть даны системы

$$\begin{aligned} (ef * \alpha), (ef * \alpha + f), (ef * \alpha + 2f), \dots, \\ (ef * \beta), (ef * \beta + f), (ef * \beta + 2f), \dots \end{aligned}$$

Произведения отдельных периодов первой системы и соответствующих периодов второй системы состоят, согласно предыдущему пункту, из целых чисел и однотипных периодов. Но небольшая внимательность при составлении этих периодов показывает, что если  $(ef * \alpha)(ef * \beta)$  состоит из целого числа  $N$  и периодов  $(ef * A), (ef * B), (ef * C), \dots$ , то произведение  $(ef * \alpha + f)(ef * \beta + f)$  будет состоять из числа  $N$  и периодов  $(ef * A + f), (ef * B + f), (ef * C + f), \dots$ , произведение  $(ef * \alpha + 2f)(ef * \beta + 2f)$  — из  $N$  и периодов  $(ef * A + 2f), (ef * B + 2f), (ef * C + 2f), \dots$ , и, вообще, произведение  $(ef * \alpha + \mu f) \times (ef * \beta + \mu f)$  — из числа  $N$  и периодов  $(ef * A + \mu f), (ef * B + \mu f), (ef * C + \mu f), \dots$ . Отсюда непосредственно вытекает, что сумма всех периодов равна

$$eN + (f * A) + (f * B) + (f * C) + \dots,$$

что и требовалось доказать.

Это доказательство также дает нам в руки способ для нахождения этой суммы.

Легко еще обобщить эту теорему, именно, в том отношении, что если имеется любое число правильно расположенных однотипных систем, и из первых, вторых и т. д. периодов образованы произведения, то сумма всех этих произведений состоит из чисел и бóльших периодов. Если все эти системы взять одинаковыми, то сумма некоторых степеней всех периодов будет состоять из чисел и периодов, однотипных с бóльшим периодом. Уже отсюда видна цель нашего исследования. Пусть  $\lambda = efgh \dots$ ; разложим все первообразные корни на  $e$  периодов  $A, A', A'', \dots$ ; каждый из них снова разложим на  $f$  периодов  $B, B', B'', \dots$ ; каждый из них — на  $g$  периодов  $C, C', C'', \dots$ . Но сумма всех периодов дана, именно, она сравнима с  $-1$ . Согласно же тому, что было только что изложено, известны также и суммы

$$\begin{aligned} & (A)^2 + (A')^2 + (A'')^2 + (A''')^2 + \dots, \\ & (A)^3 + (A')^3 + (A'')^3 + (A''')^3 + \dots, \\ & \text{и т. д.} \end{aligned}$$

Поэтому, согласно п. 244, мы можем найти сравнение  $e$ -й степени, корнями которого являются  $A, A', A'', \dots$ . Если теперь эти корни предполагаются известными, то мы разлагаем каждый период на меньшие периоды, именно,

$$\begin{aligned} A & \text{ — на } B, B', B'', \dots, \\ A' & \text{ — на } B^{(n)}, B^{(n+1)}, B^{(n+2)}, \dots, \\ A'' & \text{ — на } B^{(2n)}, B^{(2n+1)}, B^{(2n+2)}, \dots, \\ & \text{и т. д.} \end{aligned}$$

Тогда, таким образом, дано и  $B + B' + B'' + \dots \equiv A$ . Но

$$\begin{aligned} & (B)^2 + (B')^2 + (B'')^2 + \dots, \\ & (B)^3 + (B')^3 + (B'')^3 + \dots, \\ & \text{и т. д.} \end{aligned}$$

состоят из единиц и периодов  $A, A', A'', \dots$ . Поэтому  $B, B', B'', \dots$  будут задаваться сравнением  $f$ -й степени, из которого они могут быть найдены; и аналогичным образом могут быть найдены периоды, из которых состоят  $A', A'', \dots$ . Но теперь каждый может увидеть,

что совершенно аналогичным образом каждый период может быть разложен на меньшие, до тех пор, пока мы не дойдем до самих корней.

## 250

При применении этих правил имеется, однако, одна трудность, которую мы должны устранить. Именно, так как каждое сравнение имеет несколько корней, то мы должны знать, какой знак следует придавать каждому из них, чтобы можно было верно различать их один от другого. Так как значение периодов зависит от чисел  $r, \rho$ , которые могут выбираться произвольно, то и в этом вопросе обязательно остается некоторый произвол. Впрочем, число  $\rho$  должно быть с самого начала выбрано раз и навсегда. Сущность нашего метода в основном состоит в том, что мы из больших периодов получаем меньшие. Однако этого нельзя проделать без соответствующего упорядочения периодов — упорядочения, которое мы получили посредством обозначений. Поэтому мы должны постараться различать все периоды, после того как они найдены, по их знакам.

Пусть период  $A$  обозначен через  $(e * \alpha)$  и разложен на  $f$  периодов  $B, C, D, \dots$ , которые мы должны определить. Очевидно, что каждый из них будет иметь вид  $(ef * ke + \alpha)$ ; я утверждаю, однако, что для одного из них, например, для  $B$ , число  $k$  может быть выбрано произвольно, после чего уже может быть найдена последовательность остальных.

Пусть  $R$  — какой-нибудь первообразный корень сравнения  $x^n \equiv 1$ , и пусть  $B$  состоит из членов  $R^\mu + R^\nu + \dots$ ; пусть, далее,  $\frac{1}{\mu} \rho^{ke+\alpha} \equiv \frac{1}{\nu} \pmod{n}$ , и так как значение  $r$  произвольно (если только период  $A$  получает знак  $(e * \alpha)$ , что, очевидно, само по себе имеет место), то положим  $r \equiv R^\nu \pmod{p}$ . Тогда первым членом периода  $B$  будет  $r^{\rho^{ke+\alpha}}$ , и  $B$  можно обозначить через  $(ef * ke + \alpha)$ . Если бы вместо  $R^\mu$  мы рассматривали член  $R^\nu$ , то мы получили бы другое значение  $r$ ; но легко видеть, что для некоторого корня  $\rho$  корень  $r$  может иметь  $\lambda/ef$  различных значений.





Положим поэтому  $\rho = 3$  и разложим сначала все первообразные корни заданного сравнения на пять периодов, именно:

$$\begin{aligned}(5 * 0) &= (1) + (26) + (25) + (30) + (5) + (6), \\(5 * 1) &= (3) + (16) + (13) + (28) + (15) + (18), \\(5 * 2) &= (9) + (17) + (8) + (22) + (14) + (23), \\(5 * 3) &= (27) + (20) + (24) + (4) + (11) + (7), \\(5 * 4) &= (19) + (29) + (10) + (12) + (2) + (21).\end{aligned}$$

После соответствующих вычислений мы находим, что сумма периодов  $\equiv -1$ , сумма квадратов  $\equiv 25$ , сумма кубов  $\equiv 26$ , сумма би-квадратов  $\equiv 249$ , сумма пятых степеней  $\equiv 564$ .

Поэтому периоды являются корнями сравнения

$$x^5 + x^4 - 12x^3 - 21x^2 + x + 5 \equiv 0.$$

Далее мы находим

$$\begin{aligned}(5 * 0)^2 &\equiv 6 + 2(5 * 0) + * + * + 2(5 * 3) + (5 * 4), \\(5 * 0)^3 &\equiv 12 + 15(5 * 0) + 4(5 * 1) + 3(5 * 2) + 6(5 * 3) + 6(5 * 4), \\5 * 0)^4 &\equiv 90 + 60(5 * 0) + 28(5 * 1) + 26(5 * 2) + 49(5 * 3) + 38(5 * 4),\end{aligned}$$

и отсюда посредством исключения получается

$$\begin{aligned}5(5 * 1) &\equiv 3(5 * 0)^4 - (5 * 0)^3 - 33(5 * 0)^2 - 24(5 * 0) + 15, \\5(5 * 2) &\equiv -2(5 * 0)^4 - (5 * 0)^3 + 22(5 * 0)^2 + 31(5 * 0), \\5(5 * 3) &\equiv (5 * 0)^4 - 2(5 * 0)^3 + 11(5 * 0)^2 - 12(5 * 0) - 20, \\5(5 * 4) &\equiv -2(5 * 0)^4 + 4(5 * 0)^3.\end{aligned}$$

Но один из корней найденного сравнения  $\equiv 17$ ; поэтому, если положить  $(5 * 0) \equiv 17$ , то будет иметь место

$$(5 * 1) \equiv 183, (5 * 2) \equiv 263, (5 * 3) \equiv 91, (5 * 4) \equiv 67.$$

Теперь каждый из найденных периодов снова разложим на три периода, именно:

$$\begin{aligned}(5 * 0) &\text{ на } (15 * 0), (15 * 5), (15 * 10), \text{ или на } (1) + (30), (26) + (5), (25) + (6), \\(5 * 1) &\text{ на } (15 * 1), (15 * 6), (15 * 11), \text{ или на } (3) + (28), (16) + (15), (13) + (18),\end{aligned}$$

и т. д.

Если мы предположим, что

периоды, на которые разложен  $(5 * 0)$ , являются корнями сравнения

$$x^3 + Ax^2 + Bx + C \equiv 0,$$

периоды, на которые разложен  $(5 * 1)$ , являются корнями сравнения

$$x^3 + A'x^2 + B'x + C' \equiv 0,$$

периоды, на которые разложены  $(5 * 2)$ , являются корнями сравнения

$$x^3 + A''x^2 + B''x + C'' \equiv 0,$$

и т. д.,

то

$$A \equiv -(5 * 0), \quad B \equiv (5 * 0) + (5 * 3), \quad C \equiv -2 - (5 * 4),$$

$$A' \equiv -(5 * 1), \quad B' \equiv (5 * 1) + (5 * 4), \quad C' \equiv -2 - (5 * 0),$$

и т. д.

и т. д.

и т. д.

Поэтому

$(15 * 0), (15 * 5), (15 * 10)$  являются корнями сравнения

$$x^3 - 17x^2 + 108x - 69 \equiv 0,$$

$(15 * 1), (15 * 6), (15 * 11)$  » » »

$$x^3 + 128x^2 - 61x - 19 \equiv 0,$$

$(15 * 2), (15 * 7), (15 * 12)$  » » »

$$x^3 + 48x^2 - 31x + 126 \equiv 0,$$

$(15 * 3), (15 * 8), (15 * 13)$  » » »

$$x^3 - 91x^2 - 37x + 46 \equiv 0,$$

$(15 * 4), (15 * 9), (15 * 14)$  » » »

$$x^3 - 67x^2 + 19x - 93 \equiv 0.$$

Но здесь мы имеем

$$(15 * 0)^3 - 3(15 * 0) \equiv (15 * 1).$$

$$(15 * 1)^3 - 3(15 * 1) \equiv (15 * 2),$$

и т. д.

Поэтому, если положить один из корней первого сравнения, например, 10, равным  $(15 * 0)$ , то мы получаем отсюда

$$(15 * 0) \equiv 10, \quad (15 * 5) \equiv -116, \quad (15 * 10) \equiv 123,$$

$$(15 * 1) \equiv 37, \quad (15 * 6) \equiv 50, \quad (15 * 11) \equiv 96,$$

$$(15 * 2) \equiv -151, \quad (15 * 7) \equiv 139, \quad (15 * 12) \equiv -36,$$

$$(15 * 3) \equiv -39, \quad (15 * 8) \equiv 28, \quad (15 * 13) \equiv 102,$$

$$(15 * 4) \equiv -112, \quad (15 * 9) \equiv 98, \quad (15 * 14) \equiv 81.$$

Если, наконец, взять члены, которые образуют эти отдельные периоды, то

(1), (30) будут корнями сравнения  $x^2 - (15 * 0)x + 1 \equiv 0$ ,

(3), (28)       »               »               »        $x^2 - (15 * 1)x + 1 \equiv 0$ ,

и т. д.

Корнями первого сравнения являются 126 и 195; они будут тем самым первообразными корнями сравнения  $x^{31} \equiv 1$ , и остальные могут быть получены из них без труда.

---

## УЧЕНИЕ О ВЫЧЕТАХ

### II

#### Общие исследования о сравнениях

330

То, что в предыдущих разделах мы сообщили относительно сравнений, касается только простейших случаев, и по большей части находится специальными методами. В этом разделе мы хотим попытаться, насколько это в настоящее время возможно, свести теорию сравнений к более высоким принципам, приблизительно так же, как рассматривается теория уравнений, с которой, как мы уже часто отмечали, имеется значительная аналогия. Так как все алгебраические сравнения с одним неизвестным могут быть приведены к виду

$$X \equiv 0,$$

где  $X$  — алгебраическая, не содержащая дробей, функция от переменного  $x$ , то нужно главным образом рассматривать такие функции.

331

Если  $P, Q$  — функции переменного  $x$  вида

$$\begin{aligned} A + Bx + Cx^2 + Dx^3 + \dots, \\ H + Jx + Kx^2 + Lx^3 + \dots \end{aligned}$$

(в дальнейшем под простым названием «функция» всегда будут пониматься такие функции), и коэффициенты при одинаковых

степенях неизвестного  $x$  у каждой из них сравнимы по некоторому модулю, то мы будем называть функции сравнимыми по этому модулю. Очевидно, что когда для неизвестного берутся равные или сравнимые значения, то сравнимые функции будут принимать сравнимые значения. То, что в разделах I и II было доказано для чисел, в большинстве случаев имеет силу и для функций. Если, например,  $P \equiv P', Q \equiv Q', R \equiv R', \dots$ , то, очевидно, также будет иметь место  $P + Q + R + \dots \equiv P' + Q' + R' + \dots$ ;  $P - Q \equiv P' - Q'$ ;  $PQ \equiv P'Q'$ ;  $PQR \dots \equiv P'Q'R' \dots$ .

Доказательства очень легки и могут быть проведены аналогично тому, как в первом разделе.

Если  $PQ \equiv R$ , то мы будем обозначать функцию  $Q$  просто через  $R/P$ , отбрасывая модуль, и будем говорить, что  $Q$  является частным от деления  $R$  на  $P$  по этому модулю. Очевидно, однако, что вместо  $Q$  можно брать все функции, сравнимые с этой функцией, и все они будут рассматриваться в качестве одного единственного значения. В дальнейшем же мы покажем, в каких случаях такое частное может иметь несколько (несравнимых) значений.

### 332

Если модуль является простым числом, и делитель  $Q$  содержит только один член  $Hx^h$ , коэффициент которого  $H$  не делится на модуль, т. е. если  $H$  не сравнимо с 0, то частное не может иметь нескольких значений. Действительно, если бы было  $QA \equiv P$  и  $QB \equiv P$ , то имело бы место  $Q(A - B) \equiv 0$ . Если теперь

$$Q \equiv \dots + Hx^h + Jx^{h+1} + \dots,$$

где  $H$  не делится на  $p$ , и

$$A - B \equiv Lx^l + Mx^{l+1} + \dots,$$

где  $L$  не делится на  $p$  ( $A - B$  будет иметь такой вид, так как мы предполагаем, что  $A$  несравнимо с  $B$ ), то выполнялось бы сравнение  $Q(A - B) \equiv HLx^{h+l} + \dots \equiv 0$ , что невозможно, так как  $HL$  несравнимо с 0.

Теперь легко можно указать правила для деления функции  $P$  на  $Q$ , когда это возможно. Если

$$P \equiv ax^\alpha + bx^{\alpha+1} + cx^{\alpha+2} + \dots + kx^\kappa,$$

$$Q \equiv mx^\mu + nx^{\mu+1} + qx^{\mu+2} + \dots + tx^\tau,$$

где  $a, k, m, t$  не делятся на модуль, то  $\alpha$  должно быть не меньше чем  $\mu$ , и  $\kappa$  — не меньше чем  $\tau$ . Деление же может производиться аналогично тому, как в элементарной арифметике, если только все время вместо частного брать целое число, именно, частное все время будет иметь вид  $r/m$ , а это выражение по модулю имеет смысл. Если теперь, после того как найдено  $\kappa + \mu - \alpha - \tau + 1$  членов, остается остаток, который будет иметь вид

$$Ax^{\kappa+\mu-\tau+1} + Bx^{\kappa+\mu-\tau+2} + \dots + Cx^\kappa,$$

где не все коэффициенты  $A, B, C, \dots$ , сравнимы с 0, то  $P$  не может делиться на  $Q$ .

Впрочем, ясно, что деление могло бы также начинаться с членов, которые имеют наивысшие степени, т. е. с членов  $kx^\kappa, tx^\tau$ ; вычисление облегчается, если  $Q$  представить в виде

$$mx^\mu (1 + qx + rx^2 + \dots),$$

после чего, если положить  $mv \equiv 1$ , выполняется сравнение

$$\frac{P}{Q} \equiv \frac{vP : x^\mu}{1 + qx + \dots};$$

дальнейшее же деление можно производить обыкновенными методами.

### 333

**Теорема.** Если  $x \equiv a$  является корнем сравнения  $\xi \equiv 0$ , то  $\xi$  делится по модулю сравнения на  $x - a$ .

**Доказательство.** Действительно, если бы делимости не было, то имело бы место  $\xi \equiv (x - a)\xi' + b$ , где  $b$  не делится на модуль. Если положить теперь  $x \equiv a$ , то по предположению будет  $\xi \equiv 0$ , и потому  $(x - a)\xi' + b \equiv 0$ ; но при этом также и  $(x - a)\xi' \equiv 0$ , и потому обязательно  $b \equiv 0$ .

**Задача.** Пусть даны две функции; нужно найти их общий делитель (наивысшей степени) по заданному модулю.

**Решение.** Пусть даны функции  $A$  и  $B$ , и пусть  $A$  имеет такую же или бóльшую степень, чем степень  $B$ . Разделим  $A$  на  $B$ ; если деление возможно, то  $B$  является искомым общим делителем. Если же получается остаток  $C$ , то он будет степени меньшей, чем  $B$ . Пусть, таким образом,

$$A \equiv aB + C, \quad B \equiv bC + D, \quad C \equiv cD + E, \dots,$$

где  $A, B, C, D, \dots, a, b, c, \dots$  является функциями, и степени функций  $A, B, C, D, \dots$  образуют убывающий ряд. Если в конце концов какое-нибудь деление не даст остатка, например, если  $D = dE$ , то последний делитель будет искомым общим делителем; если же все время получаются остатки, то мы придем в конце концов к остатку, не имеющему степени, т. е. к числу; в этом случае функции  $A, B$  не имеют общих делителей.

**Доказательство.** Если делитель  $E$  делит предыдущую функцию без остатка, то он, как легко видеть, будет делить и все предшествующие функции; тем самым  $E$  будет общим делителем функций  $A, B$ . Это — первая часть теоремы. А если бы имелся некоторый делитель, скажем  $E'$ , большей степени, то в силу соотношения  $C \equiv A - aB$  он делил бы также и  $C$ , и по аналогичной причине делил бы  $D$  и т. д., а, значит, делил бы и  $E$ , т. е. функция более высокой степени входила бы делителем в функцию более низкой степени. Это невозможно, и потому второе утверждение доказано.

Отсюда вытекает также, что если имеется общий делитель некоторой степени, то нельзя прийти к остатку, не имеющему степени, так как иначе функция без степени делилась бы на функцию с некоторой степенью, что невозможно.

**Теорема.** Если  $A$  и  $B$  — две взаимно простые по модулю  $p$  функции, и  $A$  имеет степень  $\alpha$ , а  $B$  — степень  $\beta$ , то можно найти такие две функции  $P, Q$ , степени которых соответственно  $< \beta$  и  $< \alpha$ ,

$$PA + QB \equiv 1 \pmod{p}.$$
$$A \equiv aB + C, \quad B \equiv bC + D, \dots, \quad K \equiv kL + M,$$
$$a, a', a'', a''', \dots, a^{(x)},$$

$$1, b, b', b'', \dots, b^{(x-1)},$$
$$\begin{aligned} a' &\equiv ba + 1, & a'' &\equiv ca' + a, & a''' &\equiv da'' + a', \dots, \\ b' &\equiv cb + 1, & b'' &\equiv db' + b, & b''' &\equiv cb'' + b', \dots, \end{aligned}$$
$$A - aB \equiv + C, bA - a'B \equiv - D, b'A - a''B \equiv + E, \dots,$$
$$b^{(x-1)} A - a^{(x)} B \equiv \pm M.$$
$$PA + QB \equiv 1.$$

степень функции  $B \vdash$  степень функции  $a =$  степени функции  $A$ ,  
 »           »        $C \vdash$        »           »        $b =$        »           »        $B$ ,  
 . . . . .  
 степень функции  $L \vdash$  степень функции  $k =$  степени функции  $K$ .

степень функции  $L$  + сумма степеней функций  $a, b, c, \dots, k$  = степени функции  $A$ .

степень функции  $P$  равна  $\beta$  — степень функции  $L$ .

Это и требовалось доказать.



Но из этого следует, что если  $M$  является общим делителем наибольшей степени функций  $A, B$ , то всегда можно положить

$$AP + BQ \equiv M.$$

Примеры на предыдущую теорему я для краткости опускаю, однако для читателей было бы не лишним приобрести на таких примерах некоторую сноровку в решении подобных задач. Впрочем, стоит указать, что предыдущая теорема верна и для функций, взятых абсолютно, если их коэффициенты являются рациональными числами. Это само собой вытекает из способа доказательства. Однако мы не будем на этом задерживаться. Подобное же обстоятельство, даже и без специального указания на него, читатель заметит и в дальнейшем.

Если  $A$  не имеет общих делителей никакой степени ни с  $B$ , ни с  $C$ , то  $A$  не будет иметь общих делителей также и с произведением  $BC$ . Действительно, если  $PA + QB \equiv 1$ , то  $PAC + QBC \equiv C$ . Если бы теперь  $A$  имело бы с  $BC$  общий делитель  $M$ , то он, вопреки предположению, входил бы также и в  $C$ . Поэтому и вообще, если функция  $A$  взаимно проста с функциями  $B, C, D, \dots$ , то она будет взаимно проста и с их произведением.

Если  $A, B, C, D, \dots$  все вместе не имеют общих делителей, то можно сделать, чтобы выполнялось сравнение

$$PA + QB + RC + SD + \dots \equiv 1.$$

Если  $M$  есть делитель наивысшей степени функций  $A$  и  $B$ ,  $M'$  — делитель наивысшей степени функций  $M$  и  $C$ ,  $M''$  — делитель наивысшей степени функций  $M'$  и  $D$  и т. д., то последний член этого ряда (согласно предположению) будет, очевидно, не иметь степени. Поэтому можно положить

$$aA + bB \equiv M, \quad mM + cC \equiv M', \quad m'M' + dD \equiv M'', \dots,$$

и если произвести подстановки, мы убедимся в справедливости теоремы.

## 337

**Теорема.** Если функции  $A, B, C, \dots$  по модулю  $p$  попарно взаимно просты (т. е. никакие две из них не имеют общих делителей), и если функция  $M$  делится по этому же модулю на все эти функции в отдельности, то  $M$  делится также и на их произведение.

**Доказательство.** Можно положить  $PA + QB \equiv 1$ , и потому

$$\frac{M}{A} Q + \frac{M}{B} P \equiv \frac{M}{AB}.$$

Так как функция  $C$  взаимно проста с  $AB$ , то  $M$  будет делиться также на  $ABC$  и, по аналогичной причине, — на  $ABCD$ , и т. д.

## 338

Если сравнение  $\xi \equiv 0$  имеет корни  $x \equiv a, x \equiv b, x \equiv c, \dots$ , то  $\xi$  делится на произведение  $(x - a)(x - b)(x - c) \dots$ . Действительно, так как числа  $a, b, c, \dots$  предполагаются несравнимыми одно с другим, то функции  $x - a, x - b, x - c, \dots$  попарно взаимно просты, и так как функция  $\xi$  делится на каждую из них, она будет делиться также и на их произведение. Отсюда вытекает, что число корней не может превосходить степени сравнения. Это и есть обещанное нами доказательство этой теоремы.

Одновременно, однако, из этого усматривается, что решение сравнений образует только часть значительно более общего исследования, именно, исследования о разложении функций на сомножители. Ясно, что сравнение  $\xi \equiv 0$  не имеет вещественных корней, если  $\xi$  не обладает сомножителями *первой* степени; однако не исключено, что  $\xi$  может быть разложено на сомножители второй, третьей или более высоких степеней, вследствие чего функции  $\xi$  в известном смысле могут быть приписаны *мнимые* корни. В действительности, если бы мы пожелали воспользоваться той свободой, которую позволяют себе теперешние математики, и ввести такие мнимые величины, мы могли бы несравненно сократить наши дальнейшие исследования; тем не менее мы предпочли выводить все из старых принципов.

*Функции называются простыми по некоторому определенному модулю, если они по этому модулю не делятся ни на какие функции более низкой степени.*

Так, например, все функции первой степени простые; функции же второй степени являются либо простыми, либо составлены из двух функций *первой* степени; при этом  $\xi$  будет простой функцией второй степени, если сравнение  $\xi \equiv 0$  не имеет вещественных корней. Так, например, функция  $x^2 + x + 1$  по модулю 5 простая, потому что

$$x^2 + x + 1 \equiv (x - 2)^2 - 3 \pmod{5},$$

и 3 является квадратичным невычетом по модулю 5.

*Эти простые функции требуют нашего внимания в первую очередь.* Действительно, хотя для нахождения вещественных корней из них не могут служить никакие, кроме функций первой степени, тем не менее более подробное рассмотрение этих простых функций целесообразно как вследствие их замечательных свойств, так и потому, что из них выводятся и другие прекрасные истины.

**Теорема.** *Любая функция либо является простой, либо составлена из простых функций, причем в последнем случае она может быть составлена из простых функций только одним единственным образом.*

**Доказательство.** Именно, если заданная функция  $A$  не простая, то она будет делиться на некоторую функцию  $B$  более низкой степени. Если  $B$  — не простая функция, то она делится на некоторую другую функцию  $C$  более низкой степени, и если продолжать таким же образом, то ясно, что в конце концов мы придем к простой функции, так как в противном случае этот ряд был бы бесконечным, что невозможно, ибо степени все время убывают. Если теперь последняя простая функция есть  $L$ , то она входит делителем во все предшествующие функции. Поэтому  $A \equiv LA'$ , и  $A'$  имеет более низкую степень чем  $A$ . Но так как теперь снова  $A' \equiv L'A''$  и т. д.,

мы, очевидно, в конце концов придем к простой функции, и потому  $A$  будет сравнимо с произведением простых функций  $L, L', L'', \dots$

Если теперь предположим, что также  $A \equiv MM'M'' \dots$ , и не все функции  $L, L', L'', \dots$  совпадают с функциями  $M, M', M'', \dots$ , то отбросим те, которые являются общими для обоих рядов. Если остаются функции  $\lambda, \lambda', \lambda'', \dots; \mu, \mu', \mu'', \dots$ , то функция  $\mu$  будет взаимно проста с  $\lambda, \lambda', \lambda'', \dots$ , а потому и с их произведением  $\lambda\lambda'\lambda'' \dots$ . Несмотря на это, должно быть

$$\lambda\lambda'\lambda'' \dots \equiv \mu\mu'\mu'' \dots, \text{ т. е. } \frac{\lambda\lambda'\lambda'' \dots}{\mu} \equiv \mu'\mu'' \dots,$$

что невозможно.

### 341

Основная задача этих исследований состоит в том, чтобы *определить число простых функций каждой степени*. Именно, так как для определенного модуля число всех различных (несравнимых) функций каждой степени ограничено, а из них одни составлены из простых функций более низких степеней, а другие сами являются простыми, то и количество этих последних конечно. Строгое изложение этого предмета довольно трудно; мы начнем с более простых случаев.

Если положить модуль равным  $p$ , то число всех различных функций  $n$ -й степени вида

$$x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \dots$$

равно  $p^n$ . Действительно, число коэффициентов  $A, B, C, \dots$ , равно  $n$ , а так как каждый из них независимо от остальных может быть  $\equiv 0, 1, 2, 3, \dots, p-1 \pmod{p}$ , то из комбинаторных соображений следует, что всего имеется  $p^n$  различных комбинаций; они и будут поэтому определять совокупность всех различных функций этой степени.

Так, имеется  $p$  различных функций первой степени, именно функций  $x, x+1, x+2, \dots, x+p-1$ ;  $p^2$  различных функций второй степени и т. д.

Выше мы уже указывали на то, что все функции первой степени являются простыми; если мы ограничимся, что для нашей цели достаточно, такими функциями, старший член которых имеет коэффициент 1, то всего будет  $p$  функций первой степени.

Все функции второй степени либо составлены из двух функций первой степени, либо являются простыми. Но из комбинаторики известно, что  $p$  различных предметов можно скомбинировать по два (включая и комбинации одинаковых предметов)  $p(p+1)/1 \cdot 2$  различными способами. Поэтому столько же будет функций, составленных из двух простых функций первой степени, и потому существует  $p^2 - \frac{p(p+1)}{1 \cdot 2} = \frac{1}{2}(p^2 - p)$  простых функций второй степени.

Подобным же образом из всех функций третьей степени, число которых равно  $p^3$ , исключаются те, которые составлены из трех простых функций первой степени и число которых равно  $\frac{p(p+1)(p+2)}{1 \cdot 2 \cdot 3}$ , и, далее, исключаются те, которые составлены из простой функции первой степени и простой функции второй степени и число которых равно  $p \cdot \frac{1}{2}(p^2 - p)$ . Если их отбросить, то останется  $\frac{1}{3}(p^3 - p)$  функций; таким образом, именно столько имеется простых функций третьей степени. Очевидно, что можно и дальше продолжать подобным же образом.

Однако, чтобы легче выполнять эти операции, и одновременно проложить путь к нахождению общего закона, мы будем рассматривать вопрос в общем виде. Для краткости мы обозначим через (1) число простых функций первой степени, через (2) — число простых функций второй степени и т. д., через  $(1^2)$  — число функций, составленных из двух простых функций первой степени, и т. д., вообще, через  $(1^\alpha 2^\beta 3^\gamma \dots)$  — число всех функций, которые составлены из простых функций, причем из  $\alpha$  простых функций первой степени,  $\beta$  простых функций второй степени,  $\gamma$  простых функций третьей степени и т. д.; степень такой функции тем самым

равна  $\alpha + 2\beta + 3\gamma + \dots$ . Тогда из предыдущего и из комбинаторной теории явствует, что

$$(1^\alpha 2^\beta 3^\gamma 4^\delta \dots) = (1^\alpha) (2^\beta) (3^\gamma) (4^\delta) \dots,$$

$$(1^\alpha) = \frac{(1) [(1) + 1] [(1) + 2] [(1) + 3] \dots [(1) + \alpha - 1]}{1 \cdot 2 \cdot 3 \cdot 4 \dots \alpha},$$

или, вообще,

$$(a^\alpha) = \frac{(a) [(a) + 1] [(a) + 2] [(a) + 3] \dots [(a) + \alpha - 1]}{1 \cdot 2 \cdot 3 \cdot 4 \dots \alpha}.$$

Наконец, ясно, что если собрать все различные способы составления числа  $n$  посредством сложения из чисел  $1, 2, 3, \dots$  (эти способы можно обозначать через  $\alpha \cdot 1 + \beta \cdot 2 + \gamma \cdot 3 + \dots$ ), то сумма всех этих выражений  $(1^\alpha 2^\beta 3^\gamma \dots)$  будет равна числу всех функций степени  $n$ , т. е. равна  $p^n$ . Так, например,

$$p = (1),$$

$$p^2 = (1^2) + 2,$$

$$p^3 = (1^3) + (1 \cdot 2) + (3),$$

$$p^4 = (1^4) + (1^2 \cdot 2) + (1 \cdot 3) + (2^2) + (4),$$

и т. д.

Мы видим, что в выражение  $p^n$ , кроме величин  $(1), (2), (3), \dots$  входит также величина  $(n)$ , из чего следует, каким образом все величины могут быть определены через предшествующие. Так, мы находим

$$(1) = p, \quad (4) = \frac{1}{4} (p^4 - p^2), \quad (7) = \frac{1}{7} (p^7 - p),$$

$$(2) = \frac{1}{2} (p^2 - p), \quad (5) = \frac{1}{5} (p^5 - p), \quad (8) = \frac{1}{8} (p^8 - p^4),$$

$$(3) = \frac{1}{3} (p^3 - p), \quad (6) = \frac{1}{6} (p^6 - p^3 - p^2 + p),$$

и т. д.

Из этого начала ряда мы замечаем, что наивысший член выражения  $(n)$  равен  $p^n/n$ , и если  $n$  есть простое число, то к этому члену добавляется еще  $-p/n$ ; если же  $n$  — составное число, то за-

кон менее очевиден. Если, однако, рассмотреть положение вещей внимательнее, то мы увидим, что

$$\begin{aligned} p &= (1), & p^5 &= 5(5) + (1), \\ p^2 &= 2(2) + (1), & p^6 &= 6(6) + 3(3) + 2(2) + (1), \\ p^3 &= 3(3) + (1), & p^7 &= 7(7) + (1), \\ p^4 &= 4(4) + 2(2) + 1, & p^8 &= 8(8) + 4(4) + 2(2) + (1), \end{aligned}$$

и т. д.

где дальнейший закон уже ясен; именно, если  $\alpha, \beta, \gamma, \delta, \dots$  являются всевозможными делителями числа  $n$ , то

$$p^n = \alpha(\alpha) + \beta(\beta) + \gamma(\gamma) + \delta(\delta) + \dots$$

Мы перейдем теперь к тому, чтобы доказать общность этого замечания.

Мы показали, что сумма всех таких выражений  $(1^\alpha)(2^\beta)(3^\gamma)\dots$ , для которых  $\alpha + 2\beta + 3\gamma + \dots = n$ , исчерпывает все функции  $n$ -й степени и потому равна  $p^n$ . Отсюда вытекает — — —. Если произведение  $\left(\frac{1}{1-x}\right)^{(1)} \left(\frac{1}{1-x^2}\right)^{(2)} \left(\frac{1}{1-x^3}\right)^{(3)} \dots$  разложить в ряд  $1 + Ax + Bx^2 + \dots = P$ , то

$$\begin{aligned} A &= p, \quad B = p^2, \quad C = p^3, \dots, \\ \frac{xdP}{Pdx} &= \frac{(1)x}{1-x} + \frac{2(2)x^2}{1-x^2} + \frac{3(3)x^3}{1-x^3} + \dots, \\ \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \end{aligned}$$

(отсюда, если вместо  $\frac{xdP}{Pdx}$  подставить  $\frac{px}{1-px}$  и разложить отдельные дроби в бесконечные ряды, немедленно получается справедливость теоремы).

### 347

Эта теорема может быть выражена также и другим образом. Именно, если  $n, 1, \delta, \delta', \delta'', \delta''', \dots$  — всевозможные делители числа  $n$ , то эта теорема состоит в том, что

$$p^n = n(n) + (1) + \delta(\delta) + \delta'(\delta') + \delta''(\delta'') + \dots$$

Но очевидно, что произведение  $(n)$  простых функций, имеющих

степень  $n$ , будет иметь степень  $n(n)$ , и так же обстоит дело и для остальных произведений.

Поэтому произведение всех простых функций степеней  $1, n, \delta, \delta', \dots$  имеет степень  $p^n$ .

Теперь из этой теоремы легко вывести само значение выражения  $(n)$ ; ради краткости мы, однако, опустим вычисление, которое не трудно. Если, таким образом,  $n = a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  — различные простые числа, то

$$n(n) = p^n - \sum p^{n/a} + \sum p^{n/ab} - \sum p^{n/abc} + \dots,$$

где  $\sum p^{n/abc}$  обозначает совокупность всех выражений вида  $p^{n/abc\dots}$ , когда величины  $a, b, c, \dots$  каким-либо образом переставляются между собой. Так, например, для  $n = 36$

$$36(36) = p^{36} - p^{18} - p^{12} + p^6.$$

Мы хотим добавить еще одно замечание. Если  $n$  имеет вид  $a^\alpha$  и число  $a$  простое, то  $n(n) = p^n - p^{n/a}$ ; тем самым, так как  $(n)$  обязательно целое число, то при любом  $p$

$$p^n \equiv p^{n/a} \pmod{n},$$

и потому, если  $p$  взаимно просто с  $a$ ,

$$p^{n - \frac{n}{a}} \equiv 1 \pmod{n},$$

и для  $\alpha = 1$

$$p^{a-1} \equiv 1 \pmod{a}.$$

Замечательно, что эти теоремы могут быть получены столь различными способами.

**Задача.** Пусть дано уравнение

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \dots + M = 0,$$

корнями которого являются  $x = a, x = b, x = c, \dots$ ; нужно найти уравнение, корнями которого являются  $x = a^\tau, x = b^\tau, x = c^\tau, \dots$





рациональные, а даже целые, легко вытекает из теории уравнения  $x^\tau = 1$ .

Так как в дальнейшем мы часто будем использовать эту операцию, мы обозначим через  $(P, \rho^\tau)$  функцию, которая, будучи приравнена нулю, дает уравнение, корнями которого являются  $\tau$ -е степени корней уравнения  $P = 0$ .

Если  $P \equiv Q$  по какому-нибудь модулю, то и  $(P, \rho^\tau) \equiv (Q, \rho^\tau)$  по этому модулю.

## 349

**Теорема.** Если  $\tau$  — простое число, то коэффициент члена  $x^n$  в функции  $(P, \rho^\tau)$  сравним по модулю  $\tau$  с коэффициентом члена  $x^{n\tau}$  в функции  $P^\tau$  (что представляет собой для этого случая третье решение предыдущей задачи).

**Доказательство.** Из шестого раздела следует, что некоторый коэффициент произведения

$$(x^m + Ax^{m-1} + \dots)(x^m + A\theta x^{m-1} + \dots) \dots$$

после подстановки вместо  $\theta^\tau$  единицы принимает вид

$$E + (1 + \theta + \theta^2 + \dots + \theta^{\tau-1}) F.$$

Если теперь рассматривать  $\theta$  как первообразный корень уравнения  $x^\tau = 1$ , то все произведение обратится в  $E$ ; если же положить  $\theta = 1$ , то все произведение превращается в  $P^\tau = E + \tau F$ , и потому коэффициент члена  $x^{n\tau}$  в функции  $P^\tau$  сравним по модулю  $\tau$  с коэффициентом члена  $x^{n\tau}$  в  $E$ , т. е. с коэффициентом члена  $x^n$  в функции  $(P, \rho^\tau)$ .

## 350

**Теорема.** Если  $\tau$  — простое число, то

$$(P, \rho^\tau) \equiv P \pmod{\tau}.$$

**Доказательство.** Пусть в  $(P, \rho^\tau)$  коэффициент члена  $x^n$  равен  $N'$ , а в  $P$  коэффициент того же члена равен  $N$ . Если положить тогда

$$P = x^m + Ax^{m-1} + \dots + Nx^n + \dots,$$

то будет выполняться сравнение

$$P^\tau \equiv x^{m\tau} + A^\tau x^{(m-1)\tau} + \dots + N^\tau x^{n\tau} + \dots \pmod{\tau},$$

и потому (согласно предыдущему пункту)  $N' \equiv N^\tau \pmod{\tau}$ ; поэтому, так как  $N^\tau \equiv N$ , то и  $N' \equiv N$ , что и требовалось доказать.

Отсюда очевидно, что  $(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau})$  и  $(P, \rho^\tau) \equiv (P, \rho^{\tau^2})$ , и потому вообще

$$(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau^k}) \pmod{\tau}.$$

### 351

**Теорема.** Существует такое значение числа  $\nu < p^m$ , что функция  $x^\nu - 1$  делится по модулю  $p$  на заданную функцию  $P$  степени  $m$ , у которой низший член не содержит  $x$ .

**Доказательство.** Разделим на  $P$  ряд функций  $1, x, x^2, \dots, x^{p^m-1}$  если они имеют степени, большие чем  $m$ ; так как ни одна из этих функций не может делиться на  $P$  без остатка, то все остатки могут быть приведены к виду

$$Ax^{m-1} + Bx^{m-2} + \dots + N,$$

где все коэффициенты положительны и меньше чем  $p$ . Но ясно, что так как все коэффициенты никогда не могут быть равны 0, то имеется только  $p^m - 1$  функций, одной из которых обязательно должен быть равен каждый остаток; поэтому, так как, пока мы дойдем до степени  $x$  с показателем  $p^m - 1$ , получится  $p^m$  остатков, хотя бы два остатка обязательно должны быть равны. Пусть такие остатки получаются при делении  $x^a$  и  $x^{a+\nu}$  на  $P$ , где  $a + \nu < p^m$ . Тогда  $x^{a+\nu} - x^a$  будет делиться на  $P$ . Поэтому на  $P$  будет делиться и  $x^\nu - 1$ , так как (по предположению)  $x$ , а потому и  $x^a$  является функцией взаимно простой с  $P$ .

**Дополнение.** Если  $x^\nu - 1$  делится на  $P$ , то и  $x^{k\nu} - 1$  будет делиться на  $P$ , где  $k$  обозначает любое целое число.

### 352

**Теорема.** Пусть обозначения остаются теми же, что и в предыдущем пункте. Тогда если  $P$  — простая функция, и  $x^\nu - 1$  — наимень-

шая степень, такая, что  $x^v - 1$  делится на  $P$ , то  $v$  либо равно  $p^m - 1$ , либо является делителем этого числа, за исключением единственного случая, когда  $P \equiv x$ .

**Доказательство.** Так как  $P$  есть простая функция степени  $m$ , то существует  $p^m - 1$  различных функций степеней, меньших чем  $m$  (именно, из всех функций отбрасывается функция 0), которые все взаимно просты с  $P$ . Так как теперь, по предположению,  $x^v$  есть наименьшая степень, которая при делении на  $P$  дает остаток 1, то ясно, что если все более низкие степени от 1,  $x, \dots$  до  $x^{v-1}$  разделить на  $P$ , то получатся  $v$  различных остатков, которые мы в общем виде будем обозначать через  $A$ . Если теперь эти  $v$  остатков исчерпывают все возможные остатки, то теорема доказана; если же имеются еще остатки, не содержащиеся среди полученных, то пусть один из них есть  $B$ . Тогда очевидно, что функция  $Bx^v$  при делении на  $P$  дает остаток  $B$ , и, вообще,  $Bx^{v+k} \equiv Bx^k \pmod{P}$ . Но все функции от  $B$  до  $Bx^{v-1}$  дают остатки, отличные как один от другого, так и от остатков  $A$ ; действительно, если бы имело место  $Bx^\lambda \equiv Bx^{\lambda+\delta} \pmod{P}$ , то было бы и  $1 \equiv x^\delta \pmod{P}$ , где  $\delta < v$ , что противоречит предположению; если же было бы  $Bx^\lambda \equiv x^\mu \pmod{P}$ , то было бы также  $B \equiv x^{\mu+v-\lambda} \pmod{P}$ , и потому  $B$  совпадало бы с одним из остатков  $A$ , вопреки нашему предположению. Поэтому мы получаем, очевидно,  $v$  новых остатков. Таким же образом можно продолжать и дальше (точно так же, как и выше, в п. ...), и ясно, что число всех возможных  $p^m - 1$  остатков будет либо  $= v$ , либо  $= 2v$ , либо  $= 3v$ , т. е. вообще будет равно некоторой кратности числа  $v$ .

Из предыдущей теоремы и дополнения к п. 351 следует, что каждая простая функция степени  $n$  входит по модулю  $p$  в функцию  $x^{p^n-1} - 1$ . Поэтому все функции первой степени, за единственным исключением тех, которые сравнимы с  $x$ , будут входить в  $x^{p-1} - 1$ ; это есть теорема Ферма; все простые функции второй степени, т. е. функции вида  $x^2 + Ax + B$  будут входить в функцию  $x^{p^2-1} - 1$ , и т. д. Если теперь  $n, \delta, \delta', \delta'', \dots, 1$  суть все делители числа  $n$ ,

то очевидно, что и  $r^n - 1$  будет делиться на  $r^\delta - 1$ ,  $r^{\delta'} - 1$ ,  $r^{\delta''} - 1$ , ...,  $r - 1$ ; поэтому функция  $x^{r^n-1} - 1$  делится на все простые сомножители степеней  $n$ ,  $\delta$ ,  $\delta'$ ,  $\delta''$ , ... вплоть до простых функций первой степени (за исключением функции  $x$ ), а, значит (так как все эти функции абсолютно просты, а потому и попарно взаимно просты), также и на произведение всех этих функций. Но это произведение имеет степень  $r^n - 1$  (п. 347; одна функция,  $x$ , выбрасывается), и потому получается, что это произведение должно быть сравнимо с функцией  $x^{r^n-1} - 1$  по модулю  $r$ .

## 354

**Теорема.** Если функция  $x^v - 1$  делится на функцию  $P$ , то

$$(P, \rho^{kv+t}) \equiv (P, \rho^t),$$

где  $k, t$  обозначают любые целые числа.

**Доказательство.** Если

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \dots,$$

и если

$$\frac{mx^{m-1} + (m-1)Ax^{m-2} + \dots}{x^m + Ax^{m-1} + \dots}$$

разложить в бесконечный ряд вида

$$m \cdot \frac{1}{x} + \alpha \cdot \frac{1}{x^2} + \beta \cdot \frac{1}{x^3} + \gamma \cdot \frac{1}{x^4} + \dots,$$

то, как известно,  $\alpha$  будет суммой корней уравнения  $P = 0$ ,  $\beta$  — суммой их квадратов и т. д. Отсюда без труда выводится, что суммы  $(v+1)$ -х,  $(v+2)$ -х, ... степеней сравнимы соответственно с суммой корней, суммой их квадратов и т. д. Но из этого следует, что если только модуль не равен и не меньше степени функции  $P$ , то

$$(P, \rho^{v+1}) \equiv P, (P, \rho^{v+2}) \equiv (P, \rho^2), (P, \rho^{v+3}) \equiv (P, \rho^3), \dots$$

Оставшийся же случай мы рассмотрим ниже.

**Теорема.** Если в ряду

$$(P, \rho^0), (P, \rho^1), (P, \rho^2), (P, \rho^3), \dots$$

члены, следующие за  $\nu$ -м членом, сравнимы по порядку с первыми членами, то  $x^\nu - 1$  будет делиться на  $P$ , если только  $P$  не содержит одинаковых сомножителей.

**Доказательство.** Если положить  $\frac{dP}{dx} = Q$ , то функция  $Q$  будет взаимно проста с  $P$ . Если

$$\frac{Q}{P} = \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \dots,$$

то после члена  $N/x^\nu$  (по предположению) будет следовать

$$\frac{A}{x^{\nu+1}} + \frac{B}{x^{\nu+2}} + \frac{C}{x^{\nu+3}} + \dots$$

Поэтому

$$\frac{Q}{P} \equiv \frac{Ax^{\nu-1} + Bx^{\nu-2} + \dots}{x^\nu - 1},$$

откуда вытекает, что функция  $x^\nu - 1$  делится на  $P$ .

**Теорема.** Если  $P$  есть простая функция от  $x$  степени  $m$ , и  $X$  — функция от  $x, x^p, x^{p^2}, x^{p^3}, \dots, x^{p^{m-1}}$ , в которую все эти величины входят одинаковым образом, т. е. которая остается неизменной, каким бы образом мы эти величины не переставляли между собой, то функция  $X$  при делении на  $P$  дает остаток, являющийся числом.

**Доказательство.** Если остаток есть

$$Ax^{m-1} + Bx^{m-2} + \dots + N \equiv \xi,$$

то все коэффициенты  $A, B, C, \dots$  до  $N$ , за исключением этого последнего, будут сравнимы с 0.

Это доказывается следующим образом. Так как  $X - \xi$  делится на  $P$ , то и  $X^p - \xi^p$  делится на  $P$ . Но легко видеть, что  $X^p$  есть то,

что получается из  $X$ , если вместо  $x$  подставить  $x^p$ , вместо  $x^p$  подставить  $x^{p^2}$ , и т. д., и вместо  $x^{p^{m-1}}$  подставить  $x^{p^m}$  или, что то же самое,  $x$ . Поэтому, очевидно,  $X^p \equiv X \pmod{P}$ ; тем самым, так как  $X^p \equiv \xi^p$  и  $X \equiv \xi \pmod{P}$ , имеет место также  $\xi^p \equiv \xi \pmod{P}$ , т. е.

$$\xi^p - \xi \equiv 0 \pmod{P}.$$

Но  $\xi^p - \xi$  сравнимо по модулю  $p$  с произведением функций  $\xi, \xi + 1, \xi + 2, \dots$  до  $\xi + p - 1$ , а эти сомножители будут все взаимно просты с  $P$ , если только  $\xi$  не является просто числом. Поэтому и  $\xi^p - \xi$  ни в каком другом случае не может делиться на  $P$ .

Таковыми функциями, которые фигурируют здесь, являются сумма всех указанных величин, сумма их квадратов, кубов и т. д., суммы произведений из них по два, по три и т. д. Что представляют из себя получающиеся числа, мы определим в следующем пункте.

357

**Теорема.** Если

$$P \equiv x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \dots$$

есть простая функция предыдущего пункта, то остаток будет сравним с  $A$ , если поделить на  $P$  сумму величин  $x, x^p, \dots, x^{p^{m-1}}$ , будет сравним с  $B$ , если поделить на  $P$  сумму их произведений по два, будет сравним с  $C$ , если поделить на  $P$  сумму их произведений по три, и т. д.

**Доказательство.** Пусть указанные функции суть  $X, Y, Z, \dots$ , а их остатки по порядку суть  $A', B', C', \dots$ . Тогда легко видеть, что  $x, x^p, x^{p^2}, \dots$  являются корнями уравнения

$$z^m - Xz^{m-1} + Yz^{m-2} - Zz^{m-3} + \dots = 0.$$

Поэтому, если положить  $z = x$ , то будет выполняться равенство

$$x^m - Xx^{m-1} + Yx^{m-2} - Zx^{m-3} + \dots = 0.$$

Но функции  $X - A', Y - B', Z - C', \dots$  делятся на  $P$ , поэтому на  $P$  делится и функция

$$x^m - A'x^{m-1} + B'x^{m-2} - C'x^{m-3} + \dots$$

Это, однако, возможно только в том случае, если  $A' \equiv A$ ,  $B' \equiv B$ ,  $C' \equiv C$ , ...

Известно, кстати, что всякая другая функция  $X$  от  $x$ ,  $x^p$ ,  $x^{p^2}$ , ... (в которую все эти величины входят одинаковым образом) всегда может быть выражена через эти функции. Так, например,

$$x^2 + x^{2p} + x^{2p^2} + \dots \equiv A^2 - 2B \pmod{p}, \text{ и т. д.}$$

**Пример.** Если  $p = 5$  и  $P \equiv x^2 + 2x + 3$ , то при делении на  $P$  функция  $x + x^5$  будет сравнима с  $-2$ ,  $x^6 \equiv 3$ , и т. д.

358, 359

**Теорема.** Если  $P$  — простая функция, и  $x^v$  — наименьшая степень неизвестного  $x$ , которая при делении на  $P$  дает остаток 1, и если, далее,  $P \equiv (P, p^n)$ , то  $n$  будет сравнимо по модулю  $v$  с некоторой степенью числа  $p$ .

**Доказательство.** Выше мы показали, что если

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \dots,$$

то

$$z^m + Az^{m-1} + Bz^{m-2} + \dots - (z - x)(z - x^p) \dots (z - x^{p^{m-1}})$$

делится на  $P$ . Подобным же образом получается, что

$$z^m + Az^{m-1} + Bz^{m-2} + \dots - (z - x^n)(z - x^{np}) \dots (z - x^{np^{m-1}})$$

делится на  $P$ . Но так как эти сомножители попарно взаимно просты, то, очевидно, каждый из вторых должен быть сравним по  $P$ ,  $p$  с одним из первых. Поэтому обязательно  $z - x^n \equiv z - x^{p^x}$ , т. е.  $p^x \equiv n \pmod{v}$ . Это и требовалось доказать.

**О нахождении простых делителей функции  $x^v - 1$  по простому модулю**

360

Если  $v$  делится на модуль  $p$  или на некоторую его степень, и, скажем,  $v = p^k \cdot \lambda$ , то

$$x^v - 1 \equiv (x^\lambda - 1)^{p^k} \pmod{p}.$$



Отсюда вытекает, что нужно рассматривать только тот случай, когда  $\nu$  не делится на  $p$ .

Если  $p^m \equiv 1 \pmod{\nu}$  и при этом число  $m$  — наименьшее из возможных, то  $x^{p^m-1} - 1$  будет, очевидно, делиться на  $x^\nu - 1$ . Поэтому  $x^\nu - 1$  не может иметь других сомножителей, кроме сомножителей функции  $x^{p^m-1} - 1$ . А это выражение имеет простые делители степени  $m$  и другие делители, степени которых являются делителями числа  $m$ . Поэтому и  $x^\nu - 1$  должно иметь такие делители. Сколько делителей каждого рода имеет эта функция, мы продемонстрируем на примере, откуда легко можно будет вывести и общий закон.

Если  $\nu = 63$  и  $p = 13$ , то  $m = 6$ . Поэтому  $x^{63} - 1$  будет иметь по модулю 13 простые сомножители шестой, третьей, второй и первой степени. Но ясно, что произведение сомножителей первой степени есть общий делитель (более высокой степени) функций  $x^{63} - 1$  и  $x^{12} - 1$ , т. е. есть  $x^3 - 1$ . Поэтому имеется три сомножителя первой степени. Произведение всех простых сомножителей второй и первой степеней будет общим делителем функций  $x^{63} - 1$  и  $x^{168} - 1$ , т. е. будет равно  $x^{21} - 1$ ; поэтому имеется  $\frac{21-3}{2} = 9$  сомножителей второй степени. Произведение простых сомножителей третьей степени и первой степени будет общим делителем функций  $x^{63} - 1$  и  $x^{2196} - 1$ , т. е. равно  $x^9 - 1$ ; поэтому имеется  $\frac{9-3}{3} = 2$  делителей третьей степени. Наконец, остальные имеют шестую степень и их число, таким образом, равно  $\frac{63-6-18-3}{6}$ , т. е. равно 6.

При внимательном рассмотрении этого положения вещей мы легко получаем следующее *общее правило*.

*Пусть  $\delta$  — делитель числа  $m$ , и пусть  $\delta', \delta'', \delta''', \dots$  — всевозможные делители числа  $\delta$ , меньшие чем  $\delta$ . Пусть, далее, наибольшие общие делители числа  $\nu$  и чисел  $p^\delta - 1, p^{\delta'} - 1, p^{\delta''} - 1, \dots$  равны соответственно  $\mu, \mu', \mu'', \dots$ , и числа  $\mu/\mu', \mu/\mu'', \mu/\mu''', \dots$  равны соответственно  $\lambda', \lambda'', \lambda''', \dots$ . Тогда  $x^\nu - 1$  имеет простых делителей степени  $\delta$  в  $\delta$  раз меньше, чем имеется чисел, меньших чем  $\mu$ , которые не делятся ни на одно из чисел  $\lambda', \lambda'', \lambda''', \dots$*

## 361

**Теорема.** Если функция  $X$  от переменного  $x$  делится на другую функцию  $\xi$ , и при замене  $x$  на  $x^k$  функция  $X$  переходит в  $X'$ , то  $X'$  делится на  $(\xi, \rho^{1/k})$ .

**Доказательство.** Если  $X \equiv \xi v$  и  $\xi, v$  переходят в  $\xi', v'$ , если вместо  $x$  написать  $x^k$ , то, очевидно,  $X' \equiv \xi' v'$ . Но  $\xi'$  делится на  $(\xi, \rho^{1/k})$ , а потому делится также и  $X'$ .

## 362

После установления этих закономерностей мы можем теперь легко определить простые делители функции  $x^v - 1$ . Предположим, что все те делители, которые делят также какую-нибудь функцию  $x^{v'} - 1$ , где  $v' < v$ , уже найдены, и что нужно только получить остальные. Все они, однако, могут быть соединены в выражении  $(P, \rho^k)$ , где  $P$  есть один из них, а вместо  $k$  подставляются все числа, которые меньше чем  $v$  и взаимно просты с  $v$ .

В шестом разделе мы показали, каким образом собственные корни уравнения  $x^v = 1$  могут быть так разбиты на классы, что после того как все они будут выражены в виде степеней одного из них, в отдельных классах получается одно и то же разбиение, какой бы собственный корень ни был взят за основание. Такие совокупности корней мы будем называть периодами. Теперь ясно, что функции  $x, x^\alpha, x^\beta, x^\gamma, \dots$ , где  $\alpha, \beta, \gamma, \dots$  обозначают все взаимно простые с  $v$  числа, могут быть подобным же образом разбиты на периоды, а каждый больший период снова разбит на меньшие, пока мы в конце концов не придем к периодам вида  $x^k, x^{kp}, x^{kp^2}, \dots, x^{kp^{m-1}}$ . Если это сделано, то, очевидно,

1) так как каждый период составлен из таких наименьших периодов  $x^k + x^{kp} + \dots$ , то при делении его на некоторую простую функцию степени  $m$  в остатке получится число;

2) так как всегда все члены периода могут быть представлены в виде  $x^{x \cdot a^\alpha \cdot b^\beta \cdot c^\gamma \dots}$ , где  $x, a, b, c, \dots$  — определенные числа, а для  $\alpha, \beta, \gamma, \dots$  можно подставлять все значения, то ясно, что период переходит сам в себя, если вместо  $x$  подставить  $x^k$ , где  $k$  имеет вид  $a^\alpha b^\beta c^\gamma \dots \pmod{v}$ , откуда легко видеть, что если  $k$  обозначает

такое число, то все функции  $P, (P, \rho^k), \dots$  при делении на них периода приводят к одному и тому же остатку;

3) поэтому период после вычитания этого остатка будет делиться на произведение всех функций  $(P, \rho^k)$ .

## 363

Таким образом, в основном дело сводится к тому, чтобы определить эти остатки. Сначала определим остаток, который получается при делении на произведение всех фигурирующих здесь простых функций наибольшего периода. Если это произведение сравнимо с

$$x^\lambda - Ax^{\lambda-1} + \dots,$$

то остаток сравним с  $A$ . А вид этого произведения найти легко, и из шестого раздела получается, что  $A = 0$ , если  $\gamma$  делится на некоторый квадрат, а в противном случае,  $A$  либо равно  $+1$ , либо равно  $-1$ , в зависимости от того, четно или нечетно число простых сомножителей числа  $\gamma$ .

Разложим теперь этот наибольший период на меньшие периоды и представим периоды каждого члена через  $x^{k\rho^\pi u}$ , так что  $k$  есть для каждого периода определенное, но для различных периодов различное число, а  $\pi$  и  $u$  в каждом периоде являются переменными числами, однако те значения, которые они имеют в одном периоде, сохраняются также и в остальных. Если взять пока в качестве основания какую-нибудь простую функцию  $P$ , и если остатки от деления периодов  $\sum x^{\rho^\pi u}, \sum x^{k'\rho^\pi u}, \dots$  на  $P$  суть соответственно  $A, A', \dots$ , то  $\sum x^{\rho^\pi u} - A$  будет делиться на произведение всех функций  $(P, \rho^u)$ ,  $\sum x^{k'\rho^\pi u} - A'$  будет делиться на произведение всех функций  $(P, \rho^{k'u})$  и т. д. Но легко видеть, что величины  $A, A', \dots$  являются корнями заданного сравнения. Именно, если периоды корней уравнения  $x^\gamma - 1$ , которое соответствует предыдущим периодам, являются корнями уравнения  $Q = 0$ , то  $A, A', \dots$  будут корнями сравнения  $Q \equiv 0$ . Действительно,

$$\begin{aligned} A + A' + \dots &\equiv \text{с суммой периодов,} \\ A^2 + A'^2 + \dots &\equiv \text{с суммой квадратов периодов,} \end{aligned}$$

и т. д.

Именно, выкладки совершенно аналогичны тем, которые мы проделывали в шестом разделе, если только взять  $x$  вместо  $\rho$ , так как и здесь  $x^y$  можно заменять единицей, так же, как там  $\rho^y$ .

Если мы нашли корни  $A, A', \dots$ , то выберем какой-нибудь из них в качестве остатка периода  $\sum x^{p^u}$  и расположим затем остатки других периодов подобно тому, как мы делали это в шестом разделе. Указанный выбор здесь также произволен, так как функция  $P$  до сих пор была совершенно неопределенной. Следующая выкладка целиком аналогична той, которую мы подробно производили в шестом разделе; изложение здесь всех частных завело бы нас слишком далеко. После того как мы, наконец, придем к  $\sum x^{p^u}$ , все будет сделано. Действительно, если положить

$$P \equiv x^m + ax^{m-1} + bx^{m-2} + \dots,$$

то  $-a \equiv \sum x^{p^u}$ ; таким же образом мы получаем вторые коэффициенты остальных функций  $(P, \rho^k)$ , откуда могут быть определены другие коэффициенты функции  $P$ . Нередко может случиться, что мы будем приходить к тождественным сравнениям, из которых казалось бы ничего нельзя получить. Как можно преодолеть эту трудность, мы покажем ниже.

### 364

Все это станет намного яснее на **примере**. Пусть поставлена задача разложить на множители функцию  $x^{15} - 1$  по модулю 17. Здесь  $m = 5$ , и так как произведение всех элементарных функций сравнимо с

$$\frac{(x^{15} - 1)(x - 1)}{(x^3 - 1)(x^5 - 1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$

то имеется лишь два простых сомножителя  $P$  и  $P'$  четвертой степени. Разложим теперь  $x, x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}$  на следующие два периода:

$$\sum x^{17^\alpha} \equiv x + x^2 + x^4 + x^8,$$

$$\sum x^{7 \cdot 17^\alpha} \equiv x^7 + x^{11} + x^{13} + x^{14}.$$

Если по одной из функций  $P, P'$  имеет место

$$\sum x^{17^\alpha} \equiv A, \quad \sum x^{7 \cdot 17^\alpha} \equiv A',$$

то

$$A + A' \equiv 1,$$

$$A^2 \equiv \sum x^{2 \cdot 17^\alpha} + \sum x^{3 \cdot 17^\alpha} + \sum x^{5 \cdot 17^\alpha} + \sum x^{9 \cdot 17^\alpha},$$

$$A'^2 \equiv \sum x^{14 \cdot 17^\alpha} + \sum x^{6 \cdot 17^\alpha} + \sum x^{5 \cdot 17^\alpha} + \sum x^{3 \cdot 17^\alpha},$$

и потому

$$A^2 + A'^2 \equiv \sum x^{17^\alpha} + \sum x^{7 \cdot 17^\alpha} + 4 \sum x^{3 \cdot 17^\alpha} + 2 \sum x^{5 \cdot 17^\alpha} \equiv 1 - 4 - 4 \equiv -7.$$

Поэтому  $A, A'$  являются корнями сравнения

$$x^2 - x + 4 \equiv 0 \pmod{17},$$

и они равны 6, 12. Тем самым  $P$  будет делителем функции

$$x^8 + x^4 + x^2 + x - 6,$$

причем

$$P \equiv x^4 - 6x^3 - 2x^2 - 12x + 1.$$

Функция же  $P'$  будет сравнима с  $(P, \rho^7)$ , и потому

$$P' \equiv x^4 - 12x^3 - 2x^2 + 6x + 1.$$

### 365

Для нас достаточно здесь показать возможность этих решений. Многочисленные искусственные приемы, посредством которых эти вычисления могут быть облегчены, мы ради краткости опускаем. Напротив, мы не можем оставить без упоминания некоторые очень важные *следствия*.

Предыдущим было доказано, что все вспомогательные уравнения, для решения уравнения  $x^\nu = 1$ , будучи превращены в сравнения, имеют некоторые корни, если период

$$x + x^p + x^{p^2} + \dots + x^{p^{m-1}}$$

еще не разложен. Если мы возьмем случай, когда  $\nu$  есть простое число, то  $m$  будет делителем числа  $\nu - 1$ . Таким образом, здесь вспомогательные уравнения (если число периодов, которые при

помощи их отыскиваются, будет делителем числа  $(\nu - 1)/m$ , имеют вещественные корни. Если поэтому  $(\nu - 1)/m$  четно, т. е. если  $m$  является делителем числа  $(\nu - 1)/2$ , т. е. если  $p^{(\nu-1)/2} \equiv 1 \pmod{\nu}$ , т. е., наконец, если  $p$  является квадратичным вычетом по простому числу  $\nu$ , то квадратное уравнение, при помощи которого корни разбиваются на два периода, будет обладать вещественными корнями по модулю  $p$ . Но в шестом разделе мы показали, что если положить  $\nu = 4n \pm 1$ , то этим уравнением всегда будет  $x^2 + x \mp n = 0$ . Поэтому у нас получается следующая замечательная теорема.

**Теорема.** Если простое число  $p$  является квадратичным вычетом по простому числу  $4n \pm 1$ , то сравнение

$$x^2 + x \mp n \equiv 0 \pmod{p},$$

а потому также и сравнение

$$4x^2 + 4x \mp 4n \equiv 0 \text{ или } (2x + 1)^2 \mp \nu \equiv 0$$

будет иметь вещественные корни, т. е.  $\pm \nu$  будет квадратичным вычетом по числу  $p$ .

### 366

Это есть, таким образом, третье полное доказательство фундаментальной теоремы четвертого раздела, которое тем более замечательно, что принципы, из которых оно выведено, совершенно отличны от тех, которыми мы пользовались при прежних доказательствах. Но из этого же источника, однако, противоположным путем, мы выведем и четвертое доказательство. Именно, если  $\nu$  есть простое число вида  $4n \pm 1$ , и  $p$  — любое другое простое число, и если  $\pm \nu$  является квадратичным вычетом по простому числу  $p$ , то мы докажем, что  $p$  является квадратичным вычетом по числу  $\nu$ .

Пусть  $p^m$  — наименьшая степень числа  $p$ , которая сравнима с 1 по модулю  $\nu$ . Элементарные делители функции  $(x^\nu - 1)/(x - 1)$  по модулю  $p$  будут иметь степень  $m$ , и потому число их всех будет равно  $(\nu - 1)/m$ . Но так как  $\pm \nu R p$ , то сравнение

$$x^2 + x \mp n \equiv 0 \pmod{p}$$

разрешимо; пусть его корнями будут  $A$  и  $A'$ . Разобьем функции  $x, x^2, \dots, x^{v-1}$  на два класса, которые обозначим через  $\xi$  и  $\xi'$ ; тогда

$$\xi + \xi' \equiv A + A' + (1 + x + x^2 + \dots + x^{v-1}),$$

$$\xi\xi' \equiv AA' + \lambda(1 + x + x^2 + \dots + x^{v-1}),$$

и потому функция  $(z - \xi)(z - \xi') - (z - A)(z - A')$  будет делиться на каждый элементарный делитель функции  $(x^v - 1)/(x - 1)$ . Поэтому каждый такой элементарный делитель будет входить либо в  $\xi - A$  и  $\xi' - A'$ , либо в  $\xi - A'$  и  $\xi' - A$ . Из этого вытекает (так как  $A$  несравнимо с  $A'$ ), что если подставить  $x^p$  вместо  $x$ , то  $\xi$  и  $\xi'$  не изменятся. Действительно, если бы  $\xi$  переходило в  $\xi'$  и обратно, то  $\xi - A$  и  $\xi - A'$  делились бы на одну и ту же простую функцию, что невозможно. Отсюда следует, наконец, что  $(v - 1)/2$  делится на  $m$ , т. е.  $p^{(v-1)/2} - 1$  делится на  $v$ . Поэтому  $p$  является квадратичным вычетом по модулю  $v$ .

Все случаи фундаментальной теоремы легко вывести из каждой из этих двух теорем.

### 367

Хотя мы ограничились здесь случаем, когда  $v$  является простым числом, но аналогичные теоремы без большого труда могут быть установлены и тогда, когда число  $v$  составное, на чем, однако, мы теперь, ради краткости, подробнее останавливаться не можем.

Ясно, что подобные же замечания можно сделать также и относительно большего числа периодов. Так, если  $(v - 1)/m$  делится на 3, т. е. если  $p$  является кубическим вычетом по простому числу  $v$ , то уравнение, при помощи которого корни уравнения  $x^v = 1$  разбиваются на три периода и которое мы в шестом разделе научились определять *a priori*, будет разрешимо по модулю  $p$ , и обратно. Так, например, сравнение  $x^3 + x^2 - 2x - 1 \equiv 0$  разрешимо по любому простому модулю, который имеет вид  $7n \pm 1$ , в то время как это невозможно, если модуль имеет не такой вид.

Нам было бы не трудно обогатить эту главу еще многими другими замечаниями, если бы рамки, которыми мы должны ограни-

читься, не запрещали этого. Для тех замечаний, которые могли бы повести еще дальше, эти принципы по крайней мере смогут указать путь.

368

Мы будем говорить, что некоторое сравнение  $S \equiv 0$  имеет *равные корни*, или, более общо, *равные делители*, если  $S$  делится на степень некоторой функции.

Имеет ли заданное сравнение равные делители, можно узнавать таким же образом, как и в теории уравнений. Если положить

$$X \equiv \xi^m P,$$

то, очевидно, будет выполняться сравнение

$$\frac{dX}{dx} \equiv \xi^{m-1} \left( mP \frac{d\xi}{dx} + \xi \frac{dP}{dx} \right);$$

поэтому  $\frac{dX}{dx}$  будет делиться на  $\xi^{m-1}$ . Если вообще

$$X \equiv A^a B^b C^c \dots,$$

где  $A, B, C, \dots$  обозначают различные простые функции, то

$$\frac{dX}{dx} \equiv X \left( \frac{a}{A} \cdot \frac{dA}{dx} + \frac{b}{B} \cdot \frac{dB}{dx} + \frac{c}{C} \cdot \frac{dC}{dx} + \dots \right),$$

откуда вытекает, что если ни одно из чисел  $a, b, c, \dots$  не делится на модуль, то  $\frac{dX}{dx}$  делится на  $A^{a-1} B^{b-1} C^{c-1} \dots$ , но не делится на  $A^a, B^b, C^c, \dots$ . Из этого вытекает следующая теорема.

**Теорема.** Если общий делитель наибольшей степени функций  $X$  и  $\frac{dX}{dx}$  равен  $\xi$ , то  $X$  будет обладать всеми простыми сомножителями, которые имеет  $\xi$ , причем каждым из них в числе, на единицу большем чем  $\xi$ ; если поэтому  $X$  и  $\frac{dX}{dx}$  являются взаимно простыми функциями, то  $X$  не будет иметь равных сомножителей.



**Первый пример.** Мы хотим узнать, имеет ли функция

$$x^5 + 3x^4 - 6x^3 + 3x - 4 = X$$

равные делители по модулю 17. Имеем

$$\frac{dX}{dx} \equiv 5x^4 - 5x^3 - x^2 + 3.$$

Отсюда мы находим, что функции  $X$  и  $\frac{dX}{dx}$  взаимно просты, вследствие чего  $X$  не имеет равных сомножителей.

**Второй пример.** Если

$$X \equiv x^5 + 6x^4 - 3x^3 - 4x^2 + 2x - 3 \pmod{13},$$

то

$$\frac{dX}{dx} \equiv 5x^4 - 2x^3 + 4x^2 + 5x + 2.$$

Но наибольший общий делитель функций  $X$  и  $\frac{dX}{dx}$  сравним с  $5x^2 + 7x + 7$  или, после умножения на 8, сравним с  $x^2 + 4x + 4$ ; и так как этот делитель сравним с  $(x + 2)^2$ , то функция  $X$  будет делиться на  $(x + 2)^3$ , а частное (которое равно  $x^2 + 11$ ) уже не содержит других двойных делителей.

Если в соответствии с предыдущими пунктами функция  $X$  представлена в виде  $A^a B^b C^c \dots$ , где  $A, B, C, \dots$  — попарно взаимно простые функции, и числа  $a, b, c, \dots$  не равны 1, то разложение может продолжаться и дальше. Пусть, таким образом,  $X$  — функция, которая больше уже не содержит равных делителей. Мы видели выше, что  $x^p - x$  является произведением всех простых функций первой степени. Если  $\xi$  — общий делитель наивысшей степени функций  $X$  и  $x^p - x$ , то  $\xi$  будет произведением всех делителей первой степени функции  $X$ , и  $X/\xi$  уже не будет обладать такими делителями. Если же мы найдем, что функции  $X$  и  $x^p - x$  взаимно просты, то функция  $X$  не будет иметь делителей первой степе-

ни и потому сравнение  $X \equiv 0$  не будет иметь вещественных корней. Так как, далее,  $x^{p^2} - x$  является произведением всех простых функций второй степени и первой степени, то общий делитель наивысшей степени функций  $x^{p^2} - x$  и  $X/\xi$ , равный, скажем,  $\xi'$ , будет содержать все делители функции  $X$ , которые имеют вторую степень. Если так продолжать и дальше, то видно отсюда, что  $X$  может быть таким способом разложена на сомножители  $\xi, \xi', \xi'', \dots$ , которые содержат соответственно все делители первой, второй, третьей и т. д. степеней.

## 372

Если же дано произведение нескольких простых функций в одинаковых степенях, то отдельные функции должны определяться пробами. Эта задача имеет большое сходство с той, в которой отыскиваются сомножители составных чисел. Но здесь уже а priori определено, может ли быть заданная функция еще разложена на сомножители. Так как, кроме того, здесь количество всех возможных сомножителей конечно, мы можем пользоваться подобными же вспомогательными средствами, как и выше. Однако мы не будем задерживаться на этом вопросе, так как опытный вычислитель, свободно владеющий общими принципами, легко найдет, если это будет нужно, специальные приемы.

Мы переходим к другому вопросу, а именно, к рассмотрению сравнений, у которых модуль не является простым числом, что мы до сих пор все время предполагали. Однако здесь особенно важен случай, когда модуль является степенью простого числа, причем важен как сам по себе, так и потому, что он необходим для устранения некоторых сомнений (п. ...).

## 373

**Задача.** Пусть функция  $X$  разложена по модулю  $p$  на попарно взаимно простые сомножители  $\xi, \xi', \xi'', \dots$ ; нужно так разложить  $X$  по модулю  $p^2$  на подобные же сомножители  $\Xi, \Xi', \Xi'', \dots$ , что

$$\xi \equiv \Xi, \xi' \equiv \Xi', \xi'' \equiv \Xi'' \dots (\text{mod } p).$$

**Решение.** Если  $X \equiv \xi\psi \pmod{p}$ , т. е.  $X = \xi\psi + p\Sigma$ , и если мы положим

$$\Xi = \xi + p\varphi, \quad \Psi = \psi + p\omega,$$

то будет выполняться равенство

$$\Xi\Psi = X - p\Sigma + (\varphi\psi + \xi\omega)p + p^2\varphi\omega.$$

Если, таким образом, должно быть  $\Xi\Psi \equiv X \pmod{p^2}$ , то  $\varphi\psi + \xi\omega - \Sigma$  обязательно должно делиться на  $p$ . Но так как  $\psi$  и  $\xi$  по модулю  $p$  являются взаимно простыми функциями, то  $\varphi$  и  $\omega$  могут быть определены так, что это условие выполняется (п. 336), и притом, кроме того, так, что степени функций  $\varphi$  и  $\omega$  на единицу меньше соответственно степеней функций  $\xi$  и  $\psi$ . Тогда будет иметь место  $X \equiv \Xi\Psi \pmod{p^2}$ . Ясно, что подобным же образом  $\Psi$  снова может быть так разложена на сомножители  $\Xi'\Omega$ , что  $\Xi' \equiv \xi' \pmod{p}$ , и т. д., вследствие чего мы в конце концов получаем

$$X \equiv \Xi\Xi'\Xi'' \dots \pmod{p^2}.$$

374

После этого легко может быть доказано, что  $X$  может быть разложена на сомножители также и по модулям  $p^3, p^4, \dots$ . Если вообще

$$X \equiv PQ \pmod{p^m}, \quad \text{т. е. } X = PQ + p^m R,$$

и если функции  $P$  и  $Q$  по модулю  $p$  взаимно просты, то, полагая

$$P' = P + Ap^m, \quad Q' = Q + Bp^m,$$

мы получим

$$P'Q' = X - p^m R + (AQ + BP)p^m + ABp^{2m}.$$

Отсюда для каждого модуля  $p^\nu$  (где  $\nu > m$  и  $< 2m + 1$ ):

$$P'Q' \equiv X, \quad \text{если } R \equiv AQ + BP \pmod{p^{\nu-m}}.$$

Из этого видно, что если функция  $X$  по модулю  $p$  не имеет равных сомножителей, то она разлагается на сомножители по модулю  $p^k$  аналогично тому, как и по модулю  $p$ . Если же  $X$  имеет

равные сомножители, то дело обстоит намного сложнее, и не может быть полностью исследовано даже при помощи предыдущих принципов. Поэтому, так как мы не можем сообщить всего, что сюда относится, мы рассмотрим только один случай, который представляется важнейшим, и исследование которого нужно для разрешения некоторых оставшихся от предыдущего сомнений. Это тот случай, когда в рассмотрение входят только равные сомножители первой степени. Он может быть также целесообразно использован для нахождения корней сравнений. В другом месте мы изложим этот вопрос в общем виде.

## 375

Пусть, таким образом,  $X \equiv X' (x - a)^m \pmod{p}$ , и функция  $X'$  взаимно проста с  $x - a$ ; отыскиваются все делители функции  $X$  первой степени, которые сравнимы с делителем  $x - a$  по модулю  $p$ , а сама функция  $X$  делится на них по модулям  $p^2, p^3, \dots$  (Мы предполагаем, что абсолютно функция  $X$  не делится на  $x - a$ , так как иначе  $x - a$  делило бы функцию  $X$  по любому модулю.) Если вместо  $x$  подставить  $z + a$ , мы получим

$$Z \equiv Z' z^m \pmod{p}, \text{ или } Z = Z' z^m + pA.$$

Если теперь  $Z$  делится по модулю  $p^2$  на некоторый делитель вида  $z + \alpha p$ , то  $A$  обязательно должна иметь вид  $zZ'' + pB$ . Если это не имеет места, то исследование уже закончено. Если мы, таким образом, положим

$$Z \equiv Z' z^m + pZ'' z \pmod{p^2}, \text{ или } Z = Z' z^m + pZ'' z + p^2 B,$$

то ясно, что  $Z$  делится на  $z$  и на всякий другой делитель, сравнимый с  $z$  по модулю  $p$ .

Чтобы иметь перед собой какой-нибудь определенный случай, положим  $m = 4$ ; легко видеть, что всякий другой случай может быть изложен аналогичным образом. Если теперь  $Z$  делится по модулю  $p^3$  на некоторый делитель вида  $z + \alpha p$ , то

$$0 \equiv -\alpha p^2 Z'' + p^2 B \pmod{z + \alpha p, p^3} \text{ или } \alpha Z'' \equiv B \pmod{z, p}.$$

Теперь могут представиться три случая.

1. Если  $Z'' \equiv 0 \pmod{z, p}$ , и  $B$  не сравнимо с 0, то ясно, что ни одно значение  $\alpha$  не удовлетворяет сравнению, и потому  $Z$  не обладает по модулю  $p^3$  делителями вида  $z + \alpha p$ . Тем самым исследование закончено.

2. Если ни  $Z''$ , ни  $B$  не сравнимы с 0 по  $\pmod{z, p}$ , то  $\alpha$  будет иметь одно единственное значение, именно:

$$\alpha \equiv \frac{B}{Z''} \pmod{z, p}.$$

Поэтому будет только один делитель функции  $Z$  по модулю  $p^3$ , который сравним с  $z + \alpha p$  по модулю  $p^2$ , и будет выполняться сравнение

$$Z \equiv V(z + \alpha p) + p^3 W.$$

Если мы теперь предположим, что делителем функции  $Z \pmod{p^4}$  является  $z + \alpha p + \beta p^2$ , то

$$0 \equiv$$


---

## ДАЛЬНЕЙШЕЕ РАЗВИТИЕ ИССЛЕДОВАНИЙ О ЧИСТЫХ УРАВНЕНИЯХ

### 1

Так как метод, которым мы в «Арифметических исследованиях», п. 360, учили решать уравнение  $x^n - 1 = 0$ , образует очень плодотворную и важную теорию, для которой мы в указанном сочинении могли отметить лишь простейшие моменты, то мы надеемся, что математикам будет приятно, если мы снова вернемся к этому предмету, подробнее займемся тем, чего раньше лишь отчасти и кратко касались, опуская доказательства, и более детально исследуем то новое, что добавилось с тех пор.

Предположим, что  $n$  — простое число, а число  $n - 1$  разлагается на сомножители  $\alpha \times \beta \times \gamma$ , и обозначим, далее, через  $g$  какой-нибудь первообразный корень для модуля  $n$ . Пусть  $r$  представляет произвольный корень уравнения  $x^n - 1 = 0$ , а  $R$  — произвольный корень уравнения  $x^\beta - 1 = 0$ . Тогда если обозначить длину окружности, радиус которой равен 1, через  $P$ , и мнимую величину  $\sqrt{-1}$  через  $i$ , то все корни уравнения  $x^\beta - 1 = 0$ , т. е. все значения  $R$  будут представляться формулой

$$\cos \frac{kP}{\beta} + i \sin \frac{kP}{\beta},$$

где  $k$  пробегает все целые числа  $0, 1, 2, 3, \dots, \beta - 1$ . Далее, ясно, что все степени каждого корня  $R$  также являются корнями, и что если  $R$  есть корень, соответствующий взаимно простому с  $\beta$  значению  $k$ , то все степени  $R^0, R, R^2, R^3, \dots, R^{\beta-1}$  различны между

собой и потому исчерпывают всю совокупность корней; в этом случае мы будем называть  $R$  собственным корнем уравнения  $x^\beta - 1 = 0$ ; напротив, корень  $R$ , соответствующий не взаимно простому с  $\beta$  значению  $k$ , будет называться несобственным; если  $\delta$  есть наибольший общий делитель чисел  $k$  и  $\beta$ , то, как легко видеть,  $R^{\beta/\delta} = 1$ ; и, далее, все степени  $R^0, R, R^2, R^3, \dots, R^{\frac{\beta}{\delta}-1}$  между собой различны и потому  $R$  есть собственный корень уравнения  $x^{\beta/\delta} - 1 = 0$ . То же самое имеет место и для уравнения  $x^n - 1 = 0$ , но здесь все корни, за исключением корня 1, обязательно будут собственными корнями.

## 2

После того как предпосланы эти замечания, наше исследование будет в основном иметь дело с состоящими из  $\beta\gamma$  членов функциями следующего вида:

$$r + Rrg^\alpha + R^2rg^{2\alpha} + R^3rg^{3\alpha} + \dots + R^{\beta\gamma-1}rg^{\alpha\beta\gamma-\alpha},$$

которые мы ради краткости будем обозначать через  $[r, R]$ . Отдельные члены такого выражения являются произведениями степени числа  $r$  на степень числа  $R$ ; показатели первых образуют геометрический ряд, а показатели вторых — арифметический ряд. Все показатели

$$1, g^\alpha, g^{2\alpha}, g^{3\alpha}, \dots, g^{\alpha\beta\gamma-\alpha}$$

несравнимы по модулю  $n$ , и потому эти степени числа  $r$  различны между собой; однако, если их продолжить дальше, то начнет повторяться тот же самый ряд, так как  $g^{\alpha\beta\gamma} \equiv 1 \pmod{n}$ , и потому  $rg^{\alpha\beta\gamma} = r$ . Вторые же сомножители

$$1, R, R^2, R^3, \dots, R^{\beta\gamma-1}$$

образуют  $\gamma$  равных периодов, так как  $R^\beta = 1, R^{\beta-1} = R$  и т. д.

Из этого вытекает, что функция  $[r, R]$  может быть представлена также и в виде

или, вводя обозначение из п. 343 «Арифметических исследований»,  
в виде

3

$$\begin{aligned}[1, R] &= 1 + R + R^2 + R^3 + \dots + R^{\beta\gamma-1} = \\ &= \gamma(1 + R + R^2 + R^3 + \dots + R^{\beta-1}),\end{aligned}$$
$$[r, 1] = r + rg^{\alpha} + rg^{2\alpha} + rg^{3\alpha} + \dots + rg^{\alpha\beta\gamma-\alpha},$$

Отметим еще следующие соотношения, причина которых ясна сама собой:

где  $k$  обозначает любое положительное целое число. Отсюда вытекает, что функция  $[r^m, R]$  либо равна  $[1, R]$ , именно, если  $m$  делится на  $n$ , либо, в остальных случаях, может быть приведена к виду  $R^\mu [r^g, R]$ , и притом так, что  $\nu < \alpha$ . Действительно, если  $m$  не делится на  $n$ , то  $m$  будет сравнимо по модулю  $n$  с некоторой



степенью числа  $g$ , показатель которой, согласно «Арифметическим исследованиям», удобно обозначить через  $\text{ind } m$ ; поэтому, если положить  $\text{ind } m = \lambda\alpha + \nu$ , что, очевидно, можно сделать так, что  $\nu < \alpha$ , то

$$[r^m, R] = [r^{g^{\lambda\alpha + \nu}}, R] = R^{-\lambda} [r^{g^\nu}, R];$$

поэтому нужно положить  $\mu = -\lambda$ , или, если желательно иметь положительный показатель,  $\mu \equiv -\lambda \pmod{\beta}$ .

## 4

**Теорема.** Если  $r'$ , так же, как и  $r$ , обозначает произвольный корень уравнения  $x^n - 1 = 0$ , и, далее,  $R'$ , так же, как и  $R$ , обозначает произвольный корень уравнения  $x^\beta - 1 = 0$ , то

$$[r, R] \times [r', R'] = [rr', RR'] + R [r^{g^\alpha} r', RR'] + R^2 [r^{g^{2\alpha}} r', RR'] + \\ + R^3 [r^{g^{3\alpha}} r', RR'] + \dots + R^{\beta\gamma-1} [r^{g^{\alpha\beta\gamma-\alpha}} r', RR'].$$

**Доказательство.** Если произвести умножение  $[r, R]$  на отдельные члены функции  $[r', R']$ , то произведение можно будет представить в следующем виде:

$$[r, R] r' + RR' [r^{g^\alpha}, R] r'^{g^\alpha} + R^2 R'^2 [r^{g^{2\alpha}}, R] r'^{g^{2\alpha}} + \\ + R^3 R'^3 [r^{g^{3\alpha}}, R] r'^{g^{3\alpha}} + \dots + R^{\beta\gamma-1} R'^{\beta\gamma-1} [r^{g^{\alpha\beta\gamma-\alpha}}, R] r'^{g^{\alpha\beta\gamma-\alpha}}.$$

Если потом объединить первые члены отдельных получающихся при этом частей, то получится  $[rr', RR']$ ; если точно так же собрать вторые члены, то получится  $R [r^{g^\alpha} r', RR']$ , и т. д., откуда мы в конце концов и получаем указанный вид произведения.

Далее, простой перестановкой чисел  $r, R$  с  $r', R'$  получается, что это же произведение может быть представлено также и в следующем виде:

$$[rr', RR'] + R' [rr'^{g^\alpha}, RR'] + R'^2 [rr'^{g^{2\alpha}}, RR'] + \\ + R'^3 [rr'^{g^{3\alpha}}, RR'] + \dots + R'^{\beta\gamma-1} [rr'^{g^{\alpha\beta\gamma-\alpha}}, RR'].$$

Из этого следует далее, что если и  $r'', r''', \dots$  являются произвольными корнями уравнения  $x^n - 1 = 0$ , а  $R'', R''', \dots$  — произ-

вольными корнями уравнения  $x^\beta - 1 = 0$ , то произведение функций  $[r, R], [r', R'], [r'', R''], [r''', R'''], \dots$ , как бы велико ни было их число, равно сумме

$$\sum R'^{k'} R''^{k''} R'''^{k'''} \dots [r r'^{g^{\alpha k'}} r''^{g^{\alpha k''}} r'''^{g^{\alpha k'''}} \dots, R R' R'' R''' \dots],$$

если брать в качестве  $k', k'', k''', \dots$  всевозможные различные комбинации чисел  $0, 1, 2, 3, \dots, \beta\gamma - 1$ , вследствие чего всего получится  $\beta^{\mu-1}\gamma^{\mu-1}$  членов, если через  $\mu$  обозначено число перемножаемых функций.

## 5

Формула, которой мы в предыдущем пункте представили произведение любого числа функций, является общей и не предполагает никакой связи между корнями  $r, r', r'', r''', \dots$  или между корнями  $R, R', R'', R''', \dots$ . Отсюда без труда выводится, что так как корни  $r', r'', r''', \dots$  можно рассматривать как степени корня  $r$ , а корни  $R', R'', R''', \dots$  — как степени корня  $R$ , то отдельные части произведения могут быть приведены к виду  $R^M [r^m, R^\lambda]$ , где показатель  $\lambda$  все время один и тот же, именно  $R^\lambda = R R' R'' R''' \dots$ . Поэтому, согласно тому, что было указано в п. 3, такое произведение редуцируется к следующему виду:

$$A [1, R^\lambda] + B [r, R^\lambda] + B' [r^g, R^\lambda] + B'' [r^{g^2}, R^\lambda] + \\ + B''' [r^{g^3}, R^\lambda] + \dots + B^{(\alpha-1)} [r^{g^{\alpha-1}}, R^\lambda],$$

где отдельные коэффициенты  $A, B, B', B'', B''', \dots$  имеют вид

$$h + h' R + h'' R^2 + h''' R^3 + \dots + h^{(\beta-1)} R^{\beta-1},$$

и  $h, h', h'', h''', \dots$  обозначают определенные целые числа.

Простейшим случаем является тот, когда  $r = r' = r'' = r''' = \dots$  и  $R = R' = R'' = R''' = \dots$ ; тогда наше произведение переходит в степень  $[r, R]^\lambda$ , которая, таким образом, всегда может быть представлена в указанном выше виде.

## 6

Поэтому, если положить  $\lambda = \beta$ , то степень  $[r, R]^\beta$  примет следующий вид:

$$A[1, 1] + B[r, 1] + B'[r^g, 1] + \dots + B^{(\alpha-1)}[r^{g^{\alpha-1}}, 1] = \\ = A\beta\gamma + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \dots + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}) = \theta'.$$

Если поэтому предполагать известными не только корень  $R$  (а, значит, и значения коэффициентов  $A, B, B', \dots$ ), но и значения отдельных сумм  $(\beta\gamma, 1), (\beta\gamma, g), \dots$  из  $\beta\gamma$  членов, то тем самым немедленно будет известно значение  $\theta'$ , так что значение  $[r, R]$  можно будет найти по формуле  $\sqrt[\beta]{\theta'}$ . Это выражение допускает  $\beta$  различных значений, так что могла бы возникнуть неопределенность в отношении того, какое из них следует брать; но легко показать, что это совершенно безразлично, если  $R$  является собственным корнем уравнения  $x^\beta - 1 = 0$ . Действительно, в этом случае указанными  $\beta$  значениями корня  $\sqrt[\beta]{\theta'}$  будут, очевидно, следующие значения:

$$[r, R], [r^{g^\alpha}, R], [r^{g^{2\alpha}}, R], \dots, [r^{g^{\alpha\beta-\alpha}}, R],$$

ибо  $\beta$ -е степени этих функций, согласно п. 3, равны между собой, а сами эти функции пропорциональны  $\beta$  различным корням уравнения  $x^\beta - 1 = 0$ . Если же известны только суммы  $(\beta\gamma, 1), (\beta\gamma, g), \dots$  из  $\beta\gamma$  членов, то сам корень  $r$  определен лишь в том смысле, что он должен содержаться в совокупности  $(\beta\gamma, 1)$ , и остается произвольным, какой из корней этой совокупности берется за  $r$ . Но эти корни суть  $r, r^{g^\alpha}, r^{g^{2\alpha}}, \dots$ , и потому из функций  $[r, R], [r^{g^\alpha}, R], [r^{g^{2\alpha}}, R], \dots$  мы тоже можем любую взять в качестве  $[r, R]$ .

Эти заключения не имели бы силы, если бы  $R$  не было собственным корнем уравнения  $x^\beta - 1 = 0$ . Действительно, если предположить, что  $R$  является собственным корнем уравнения  $x^{\beta'} - 1 = 0$ , где  $\beta'$  есть делитель числа  $\beta$ , то легко получается, что

$$[r, R] = [r^{g^{\alpha\beta'}}, R], [r^{g^\alpha}, R] = [r^{g^{\alpha\beta'+\alpha}}, R], \dots,$$

и потому в совокупности из  $\beta$  функций  $[r, R], [r^g, R], \dots, [r^{g^{\alpha\beta-\alpha}}, R]$  будет только  $\beta'$  различных, т. е. из значений выражения  $\sqrt[\beta]{\theta'}$  допустимы не более чем  $\beta'$  значений, остальные  $\beta - \beta'$  значений должны быть отброшены. Но легко видеть, что в этом случае не нужно доходить до  $\beta$ -й степени функции  $[r, R]$ , а что уже  $[r, R]^{\beta'}$  приводится к нашему виду

$$\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \dots$$

Мы получаем поэтому  $[r, R]$  в виде выражения  $\sqrt[\beta']{\theta'}$ , и безразлично, какое значение этого выражения мы берем.

## 7

Так же, как  $[r, R]$ , можно определить и функции  $[r, R^2], [r, R^3], \dots$ , или вообще  $[r, R^k]$ ; действительно, если мы предположим, что при подстановке в  $\theta'$  вместо  $R$  степеней  $R^2, R^3, \dots, R^k$  получаются функции  $\theta'', \theta''', \dots, \theta^{(k)}$ , то, очевидно, будет иметь место  $[r, R^2]^\beta = \theta'', [r, R^3]^\beta = \theta''', \dots$ , и вообще  $[r, R^k]^\beta = \theta^{(k)}$ , вследствие чего и эти функции могут быть представлены в виде корней:  $[r, R^2] = \sqrt[\beta]{\theta''}$  и т. д. Однако, если какую-нибудь величину нужно выразить через одну из функций  $[r, R], [r, R^2], \dots$ , то эти выражения в виде корней использовать не целесообразно. Именно, так как значения отдельных корней не вполне определены, то оставалась бы неопределенность в том, какие значения можно комбинировать между собой, а это, очевидно, не безразлично; действительно, легко видеть, что если для  $[r, R]$  взято определенное значение, то и все функции  $[r, R^2], [r, R^3], \dots$  должны получить вполне определенные значения, которые, однако, не указываются выражениями через корни. Поэтому эти выражения нужно отбросить и найти другие, при помощи которых  $[r, R^2], [r, R^3], \dots$  рационально представляются через  $[r, R]$  и известные величины; это легко достигается следующим образом.

Согласно теореме п. 4 и тому, что было изложено в п. 5, произведение  $[r, R^k] \times [r, R]^{\beta-k}$  тоже может быть представлено в

таком виде:

$$\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \dots + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}),$$

где  $A, B, B', B'', \dots$  будут рациональными функциями от  $R$ . Поэтому, если положить

$$[r, R^2] \times [r, R]^{\beta-2} = \theta'',$$

$$[r, R^3] \times [r, R]^{\beta-3} = \theta''',$$

$$[r, R^4] \times [r, R]^{\beta-4} = \theta''''$$

и т. д.,

то  $\theta'', \theta''', \theta''', \dots$  также будут рационально заданными величинами, и будут выполняться равенства

$$[r, R^2] = \frac{\theta''}{\theta'} [r, R]^2,$$

$$[r, R^3] = \frac{\theta'''}{\theta'} [r, R]^3,$$

$$[r, R^4] = \frac{\theta''''}{\theta'} [r, R]^4$$

и т. д.

Таким образом, эти выражения рационально представляют значения функций  $[r, R^2], [r, R^3], \dots$ , если только  $[r, R]$  не равно 0, когда они будут неопределенны; мы можем, однако, строго доказать, что никогда не может быть  $[r, R] = 0$ , по крайней мере если  $r$  обозначает корень, отличный от 1, хотя изложение этого доказательства мы, чтобы не быть здесь слишком пространными, должны отложить до другого случая.

## 8

Рассмотрение предыдущего пункта оказывается полезным, если поставлена задача спуститься от периодов из  $\beta\gamma$  членов к периодам из  $\gamma$  членов. Действительно, легко видеть, что если  $R$  обозначает собственный корень, то мы получаем

$$\beta(\gamma, 1) = (\beta\gamma, 1) + [r, R] + [r, R^2] + [r, R^3] + \dots + [r, R^{\beta-1}],$$

$$\begin{aligned} \beta(\gamma, g^\alpha) = (\beta\gamma, 1) + R^{\beta-1}[r, R] + R^{\beta-2}[r, R^2] + R^{\beta-3}[r, R^3] + \dots \\ \dots + R[r, R^{\beta-1}], \end{aligned}$$

$$\beta(\gamma, g^{2\alpha}) = (\beta\gamma, 1) + R^{2\beta-2}[r, R] + R^{2\beta-4}[r, R^2] + R^{2\beta-6}[r, R^3] + \dots \\ \dots + R^2[r, R^{\beta-1}]$$

и т. д.

Если бы здесь для отдельных функций  $[r, R]$ ,  $[r, R^2]$ , ... были взяты их выражения в виде корней  $\sqrt[\beta]{\theta'}$ ,  $\sqrt[\beta]{\theta''}$ , ..., то значение каждого ряда определялось бы лишь с точностью до  $\beta^{\beta-1}$  различных значений, в то время как, когда мы берем для  $[r, R^2]$ , ... рациональные выражения, то не остается уже никакой неопределенности, кроме тех неопределенностей, которые неизбежны по самой природе вопроса. Это замечание ускользнуло от внимания Лагранжа, считавшего, что указанный нами в п. 360 «Арифметических исследований» метод, где мы умышленно пользовались только рациональными выражениями и не употребляли выражений в виде корней, можно было бы упростить, подставив вторые вместо первых («*Traité de la résolution numérique des équations*», édition 2-ième, p. 311).

Далее, вряд ли даже необходимо указывать на то, что как только получены значения периодов  $(\gamma, 1)$ ,  $(\gamma, g^\alpha)$ , ... или только одного из них, то отсюда уже могут быть рациональным образом получены значения всех остальных периодов из  $\gamma$  членов. Поэтому спуск от периодов с  $\beta\gamma$  членами к периодам с  $\gamma$  членами требует решения уравнений  $x^\beta = 1$ ,  $x^\beta = \theta'$ , а все остальные операции выполняются рационально.

## 9

Все это почти таким же образом рассматривалось в «Арифметических исследованиях»: однако кое-что там было сообщено без доказательств, привести которые здесь является бесполезным. Мы утверждали там, что нахождение значения корня  $\sqrt[\beta]{\theta'}$ , которое, по крайней мере тогда, когда  $\theta'$  является мнимой величиной, на первый взгляд требует деления на  $\beta$  частей как некоторого отрезка, так и некоторого угла, на самом деле зависит только от последнего, а первое всегда может быть сведено к извлечению одного квадратного корня. Это мы докажем следующим образом.

Если, как и выше, обозначить мнимую величину  $\sqrt{-1}$  через  $i$  и положить  $\theta' = P + iQ$ , а какое-нибудь значение выражения  $\sqrt[\beta]{\theta'}$  положить равным  $p + iq$ , где  $P, Q, p, q$  вещественны, то, как известно, если положительные величины  $E, e$  и углы  $F, f$  определены так, что

$$P = E \cos F, \quad Q = E \sin F, \quad p = e \cos f, \quad q = e \sin f,$$

то

$$e = \sqrt[\beta]{E},$$

и  $f$  равен одному из углов

$$\frac{1}{\beta} F, \quad \frac{1}{\beta} (F + 360^\circ), \quad \frac{1}{\beta} (F + 720^\circ), \dots, \quad \frac{1}{\beta} (F + (\beta - 1) 360^\circ).$$

Поэтому  $f$  будет определяться делением угла  $F$  на  $\beta$  частей, а извлечения корня  $\sqrt[\beta]{E}$  мы можем избежать следующим образом. Каждое произведение  $r^k R^K$  имеет одинаковую вещественную часть с  $r^{-k} R^{-K}$ , а мнимые части, содержащие множитель  $i$ , у этих произведений равны по величине, но противоположны по знаку. Отсюда немедленно следует, что

$$[r^{-1}, R^{-1}] = p - iq = e (\cos f - i \sin f),$$

и потому

$$[r, R] \times [r^{-1}, R^{-1}] = e^2.$$

Но указанное произведение, согласно теореме п. 4, равно

$$\begin{aligned} & [1, 1] + R [r^{g^\alpha - 1}, 1] + R^2 [r^{g^{2\alpha} - 1}, 1] + \dots + R^{\beta\gamma - 1} [r^{g^{\alpha\beta\gamma - \alpha} - 1}, 1] = \\ & = \beta\gamma + R(\beta\gamma, g^\alpha - 1) + R^2(\beta\gamma, g^{2\alpha} - 1) + \dots + R^{\beta\gamma - 1}(\beta\gamma, g^{\alpha\beta\gamma - \alpha} - 1), \end{aligned}$$

а эти величины можно определить, если  $R$  и все периоды из  $\beta\gamma$  членов предполагаются известными. Таким образом, определение  $e$  требует только извлечения квадратного корня.

В специальном случае, когда  $\alpha = 1$ , отдельные периоды  $(\beta\gamma, g^\alpha - 1)$ ,  $(\beta\gamma, g^{2\alpha} - 1)$ ,  $\dots$ , очевидно, равны  $r + r^2 + r^3 + r^4 + \dots + r^{n-1}$ , и потому

$$e^2 = \beta\gamma + (R + R^2 + R^3 + \dots + R^{\beta\gamma-1})(r + r^2 + r^3 + \dots + r^{n-1}) = \\ = \beta\gamma + 1 = n,$$

если считать, что  $r$  и  $R$  представляют собой корни, отличные от 1, и потому всегда  $e = \sqrt[n]{n}$  («Арифметические исследования», в конце п. 360).

## 10

До сих пор мы проводили наше исследование во всей общности, так что охватывали любые значения чисел  $\alpha$ ,  $\beta$ ,  $\gamma$ ; однако, начиная отсюда, мы переходим к более специальному случаю  $\alpha = 1$ , который проложит нам путь к плодотворнейшему и изящнейшему исследованию.

Пусть поэтому знак  $[r, R]$  представляет функцию

$$r + Rr^g + R^2r^{g^2} + R^3r^{g^3} + \dots + R^{n-2}r^{g^{n-2}},$$

где  $n$  — простое число,  $r$  — произвольный корень уравнения  $x^n - 1 = 0$  (не исключая и корня 1),  $R$  — произвольный корень уравнения  $x^\beta - 1 = 0$ ; далее,  $\beta$  обозначает некоторый заданный делитель числа  $n - 1$ , и, наконец,  $g$  — некоторый определенный первообразный корень для модуля  $n$ . Далее, мы положим ради краткости

$$1 + r + r^2 + r^3 + \dots + r^{n-1} = s, \\ 1 + R + R^2 + R^3 + \dots + R^{n-2} = S,$$

откуда следует, что  $s = n$  для  $r = 1$  и  $s = 0$  для всякого другого значения  $r$ , и точно так же  $S = n - 1$  для  $R = 1$ , но  $S = 0$  для любого другого значения  $R$ .

Тем самым, согласно п. 3, мы имеем

$$[1, R] = S, \quad [r, 1] = s - 1;$$

далее, для каждого не делящегося на  $n$  значения  $m$

$$[r^m, R] = R^{-\text{ind } m} [r, R],$$



или более общо

$$[r^m, R^M] = R^{-M \operatorname{ind} m} [r, R^M],$$

где  $\operatorname{ind} m$  обозначает показатель степени числа  $g$ , сравнимой по модулю  $n$  с  $m$ . Если мы применим это преобразование к тому, о чем говорилось в п. 5, то мы получим, что произведение двух или большего числа сомножителей вида  $[r^h, R^H]$  приводится к виду

$$A [1, R^\lambda] + B [r, R^\lambda],$$

где  $A$  и  $B$  являются рациональными функциями от  $R$  с целыми коэффициентами, а  $\lambda$  есть сумма всех значений  $H$ . Очень важно свести такие преобразования к простому алгоритму; для этой цели мы должны, в частности, подробнее рассмотреть природу произведения двух функций.

# 11

Произведение  $[r, R^\mu] \times [r, R^\nu]$ , согласно теореме п. 4, равно

$$[r^2, R^{\mu+\nu}] + R^\mu [r^{g+1}, R^{\mu+\nu}] + R^{2\mu} [r^{g^2+1}, R^{\mu+\nu}] + \\ + R^{3\mu} [r^{g^3+1}, R^{\mu+\nu}] + \dots + R^{(n-2)\mu} [r^{g^{n-2}+1}, R^{\mu+\nu}].$$

Из  $n-1$  показателей  $2, g+1, g^2+1, \dots, g^{n-2}+1$  здесь встречается только один делящийся на  $n$ , именно, показатель  $g^{(n-1)/2}+1$ ; соответствующий член нашей суммы будет, таким образом, равен

$$R^{(n-1)\mu/2} [1, R^{\mu+\nu}];$$

этот член равен 0, если  $R^{\mu+\nu}$  не равно 1, и равен  $(n-1) R^{(n-1)\mu/2} = \pm (n-1)$  для  $R^{\mu+\nu} = 1$ . Остальные части нашего выражения, сумму которых мы положим равной  $\Omega$ , преобразуются следующим образом:

$$[r^2, R^{\mu+\nu}] = R^{-(\mu+\nu) \operatorname{ind} 2} [r, R^{\mu+\nu}], \\ R^\mu [r^{g+1}, R^{\mu+\nu}] = R^{\mu-(\mu+\nu) \operatorname{ind} (g+1)} [r, R^{\mu+\nu}], \\ R^{2\mu} [r^{g^2+1}, R^{\mu+\nu}] = R^{2\mu-(\mu+\nu) \operatorname{ind} (g^2+1)} [r, R^{\mu+\nu}], \\ R^{3\mu} [r^{g^3+1}, R^{\mu+\nu}] = R^{3\mu-(\mu+\nu) \operatorname{ind} (g^3+1)} [r, R^{\mu+\nu}]$$

и т. д.

Отсюда вытекает, что

$$\text{I. } \Omega = [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } x - (\mu+\nu) \text{ ind } (x+1)},$$

если вместо  $x$  подставлять последовательно значения  $1, g, g^2, g^3, \dots, g^{n-2}$ , исключая только значение  $g^{(n-1)/2}$ , или, что то же самое, если вместо  $x$  подставлять значения  $1, 2, 3, 4, \dots, n-2$ , так как вторые значения сравнимы с первыми (быть может только в другом порядке) по модулю  $n$ .

Если мы предположим, что целое число  $y$  является обратным для  $x$  по модулю  $n$ , т. е. определено так, что  $xy \equiv 1 \pmod{n}$ , то будет иметь место  $\text{ind } x \equiv -\text{ind } y \pmod{n-1}$  и

$$\text{ind } (x+1) + \text{ind } y \equiv \text{ind } (xy+y) \equiv \text{ind } (1+y) \pmod{n-1}.$$

Поэтому

$$\begin{aligned} \mu \text{ ind } x - (\mu + \nu) \text{ ind } (x+1) &\equiv -\mu \text{ ind } y - (\mu + \nu) \{\text{ind } (y+1) - \text{ind } y\} \equiv \\ &\equiv \nu \text{ ind } y - (\mu + \nu) \text{ ind } (y+1). \end{aligned}$$

А так как числа, обратные к числам  $1, 2, 3, \dots, n-2$ , совпадают с ними, только расположены в другом порядке, то

$$\text{II. } \Omega = [r, R^{\mu+\nu}] \times \sum R^{\nu \text{ ind } y - (\mu+\nu) \text{ ind } (y+1)},$$

если вместо  $y$  подставлять последовательно числа  $1, 2, 3, \dots, n-2$ . Эта же формула немедленно получается и из I, так как числа  $\mu, \nu$ , очевидно, можно поменять местами.

Если, наконец, предположить, что целое число  $z$  является обратным по модулю  $n$  для  $x+1$ , т. е.  $xz + z \equiv 1 \pmod{n}$ , то

$$\begin{aligned} \text{ind } (1-z) &\equiv \text{ind } x + \text{ind } z \pmod{n-1}, \\ \text{ind } (x+1) &\equiv -\text{ind } z \pmod{n-1}, \end{aligned}$$

и потому

$$\begin{aligned} \mu \text{ ind } x - (\mu + \nu) \text{ ind } (x+1) &\equiv \mu [\text{ind } (1-z) - \text{ind } z] + (\mu + \nu) \text{ ind } z \equiv \\ &\equiv \mu \text{ ind } (1-z) + \nu \text{ ind } z. \end{aligned}$$

Так как когда  $x$  пробегает значения  $1, 2, 3, \dots, n-2$ , число  $z$  должно пробегать (быть может только в другом порядке) значения  $2, 3, 4, \dots, n-1$ , мы получаем тем самым третье выражение

$$\text{III. } \Omega = [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } (1-z) + \nu \text{ ind } z},$$

где вместо  $z$  последовательно подставляются числа  $2, 3, 4, \dots, n-1$ , или, если угодно, выражение

$$\begin{aligned}\Omega &= [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } (n+1-z) + \nu \text{ ind } z} = \\ &= [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } z + \nu \text{ ind } (n+1-z)}.\end{aligned}$$

Так как  $\text{ind}(1-z) = \frac{1}{2}(n-1) + \text{ind}(z-1)$ , то наше произведение можно представить и так:

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] &= R^{(n-1)\mu/2} \{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } (z-1) + \nu \text{ ind } z}\} = \\ &= R^{(n-1)\nu/2} \{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \sum R^{\mu \text{ ind } z + \nu \text{ ind } (z-1)}\},\end{aligned}$$

где все время числами, подставляемыми вместо  $z$ , являются числа  $2, 3, 4, \dots, n-1$ .

Заметим, что во всех этих формулах вместо чисел

$$\begin{aligned}\mu \text{ ind } x - (\mu + \nu) \text{ ind } (x+1), \quad \nu \text{ ind } y - (\mu + \nu) \text{ ind } (y+1), \\ \mu \text{ ind } (1-z) + \nu \text{ ind } z, \text{ и т. д.}\end{aligned}$$

можно, очевидно, подставлять их наименьшие вычеты по модулю  $\beta$ .

Если  $\mu + \nu \equiv 0 \pmod{\beta}$ , то

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] &= (n-1) R^{(n-1)\mu/2} + (r + r^2 + r^3 + \dots + r^{n-1}) \times \\ &\times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \dots + R^{(n-2)\mu} - R^{(n-1)\mu/2}).\end{aligned}$$

## 12

Произведение  $[1, R^{\mu}] \times [r, R^{\nu}]$ , согласно теореме п. 4, равно

$$\begin{aligned}[r, R^{\mu+\nu}] + R^{\mu} [r, R^{\mu+\nu}] + R^{2\mu} [r, R^{\mu+\nu}] + \dots + R^{(n-2)\mu} [r, R^{\mu+\nu}] = \\ = [r, R^{\mu+\nu}] \times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \dots + R^{(n-2)\mu}) = \\ = [r, R^{\mu+\nu}] \times \frac{n-1}{\beta} (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \dots + R^{(\beta-1)\mu}).\end{aligned}$$

Поэтому произведение  $[1, R^{\mu}] \times [1, R^{\nu}]$  может быть преобразовано в

$$\frac{n-1}{\beta} [1, R^{\mu+\nu}] \times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \dots + R^{(\beta-1)\mu}).$$

Теперь без труда можно получить и любое произведение  $[r^m, R^\mu] \times [r^{m'}, R^{\mu'}]$ ; действительно, так как  $[r^m, R^\mu] = R^{-\mu \text{ ind } m} [r, R^\mu]$  для не делящегося на  $n$  значения  $m$ , и равно  $[1, R^\mu]$  для делящегося на  $n$  значения  $m$ , и так как подобное же преобразование сохраняет силу и для других сомножителей  $[r^{m'}, R^{\mu'}]$ , то умножение сводится или к задаче предыдущего пункта, или к тем случаям, которые мы рассматривали в настоящем пункте.

## 13

После того как мы показали, как преобразовывать произведение двух сомножителей, преобразование произведения нескольких сомножителей уже не представляет труда. Если произведение  $[r, R^\mu] \times [r, R^\nu]$  приведено к виду  $A[1, R^{\mu+\nu}] + B[r, R^{\mu+\nu}]$ , то ясно, что если добавить третий сомножитель  $[r, R^\pi]$ , произведение будет равно  $C[1, R^{\mu+\nu+\pi}] + D[r, R^{\mu+\nu+\pi}]$ , где положено

$$[r, R^{\mu+\nu}] \times [r, R^\pi] = c[1, R^{\mu+\nu+\pi}] + d[r, R^{\mu+\nu+\pi}],$$

и

$$C = Bc, \quad D = Bd + A\{1 + R^{\mu+\nu} + R^{2\mu+2\nu} + \dots + R^{(n-2)(\mu+\nu)}\}.$$

Поэтому  $[r, R]^\lambda$  легко может быть приведено к виду

$$A[1, R^\lambda] + B[r, R^\lambda].$$

Ради примера мы найдем степени функции  $[r, R]$  для  $n = 11$ ,  $\beta = 5$ , причем мы положим  $g = 2$ . Здесь числам

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

соответствуют индексы

$$0, 1, 8, 2, 4, 9, 7, 3, 6, 5.$$

Поэтому для разложения квадрата  $[r, R]^2$  по формуле I п. 11 мы имеем

$$\mu = 1, \quad \nu = 1.$$

|                                                                   |                                 |
|-------------------------------------------------------------------|---------------------------------|
| Значения $x$ . . . . .                                            | 1, 2, 3, 4, 5, 6, 7, 8, 9.      |
| $\text{ind } x$ . . . . .                                         | 0, 1, 8, 2, 4, 9, 7, 3, 6.      |
| $2 \text{ ind } (x + 1)$ . . . . .                                | 2, 16, 4, 8, 18, 14, 6, 12, 10. |
| Наименьший вычет                                                  |                                 |
| числа $\text{ind } x - 2 \text{ ind } (x + 1) \pmod{5}$ . . . . . | 3, 0, 4, 4, 1, 0, 1, 17, 1,     |

откуда мы получаем

$$\Omega = [r, R^2] \times \{2 + 4R + R^3 + 2R^4\},$$

и

$$1) [r, R]^2 = [1, R^2] + [r, R^2] \times \{2 + 4R + R^3 + 2R^4\}.$$

То же самое выражение получается из формулы III п. 11, именно

|                                                                    |                             |
|--------------------------------------------------------------------|-----------------------------|
| Значения $z$ . . . . .                                             | 2, 3, 4, 5, 6, 7, 8, 9, 10. |
| $\text{ind } z$ . . . . .                                          | 1, 8, 2, 4, 9, 7, 3, 6, 5.  |
| $\text{ind } (n + 1 - z)$ . . . . .                                | 5, 6, 3, 7, 9, 4, 2, 8, 1.  |
| Наименьший вычет                                                   |                             |
| числа $\text{ind } z + \text{ind } (n + 1 - z) \pmod{5}$ . . . . . | 1, 4, 0, 1, 3, 1, 0, 4, 1.  |

Совершенно аналогичным образом мы находим

$$\begin{aligned} 2) [r, R^2] \times [r, R] &= [1, R^3] + [r, R^3] \times \{2 + R + 4R^2 + 2R^3\}, \\ 3) [r, R^3] \times [r, R] &= [1, R^4] + [r, R^4] \times \{2 + 4R + R^3 + 2R^4\}. \end{aligned}$$

Наконец,

$$4) [r, R^4] \times [r, R] = [1, 1] + [r, 1] \times \{1 + 2R + 2R^2 + 2R^3 + 2R^4\}.$$

Если умножить равенство 1) на  $[r, R]$  и подставить вместо  $[r, R^2] \times [r, R]$  его значение из 2) и далее подставить

$$[1, R^2] \times [r, R] = [r, R^3] \times \{2 + 2R + 2R^2 + 2R^3 + 2R^4\},$$

то мы получим равенство

$$\begin{aligned} [r, R]^3 &= [1, R^3] \times \{2 + 4R + R^3 + 2R^4\} + \\ &+ [r, R^3] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\}, \end{aligned}$$

и точно так же

$$\begin{aligned} [r, R]^4 &= [1, R^4] \times \{12 + 22R + 18R^2 + 24R^3 + 15R^4\} + \\ &+ [r, R^4] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\}. \\ [r, R]^5 &= [1, 1] \times \{164 + 170R + 205R^2 + 180R^3 + 190R^4\} + \end{aligned}$$

$$\begin{aligned}
& + [r, 1] \times \{1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4\} = \\
& = 1640 + 1700R + 2050R^2 + 1800R^3 + 1900R^4 + \\
& + (1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4)(s-1) = \\
& = 918Ss - 98S - (6R + 41R^2 + 16R^3 + 26R^4)s + \\
& + 66R + 451R^2 + 176R^3 + 286R^4.
\end{aligned}$$

## 14

Вычисления, которые до сих пор проводились таким образом, что они были пригодны для всех значений  $r$  и  $R$ , могут быть значительно сокращены, если мы с самого начала будем рассматривать  $R$  как собственный корень уравнения  $x^\beta - 1 = 0$ . При этом предположении произведение  $[r, R^\mu] \times [r, R^\nu]$  преобразуется к виду  $B[r, R^{\mu+\nu}]$ , если только  $\mu + \nu$  не делится на  $\beta$ . Если же  $\mu + \nu$  делится на  $\beta$ , то указанное произведение будет равно  $(n-1)R^{(n-1)\mu/2} + [r, 1] \sum R^{\text{ind } x}$ , если вместо  $\text{ind } x$  подставлять все значения  $0, 1, 2, 3, \dots, n-2$ , за исключением значения  $(n-1)/2$ . Отсюда легко видеть (если  $\mu$ , а потому также и  $\nu$  не делится на  $\beta$ ), что в этом случае

$$[r, R^\mu] \times [r, R^\nu] = R^{(n-1)\mu/2} \{n-1 - [r, 1]\},$$

и потому  $[r, R^\mu] \times [r, R^\nu]$  равно 0 для  $r=1$ , и равно  $nR^{(n-1)\mu/2}$  для всякого другого значения  $r$ . Так как, далее,  $R^{(n-1)\mu/2} = +1$  или  $= -1$ , в зависимости от того, является ли число  $(n-1)\mu/\beta$  четным или нечетным, то наше произведение в первом случае будет равно  $n$ , а во втором равно  $-n$ .

Далее, из этого следует, что можно положить

$$\begin{aligned}
[r, R]^2 &= A' [r, R^2], \\
[r, R^2] \times [r, R] &= A'' [r, R^3], \\
[r, R^3] \times [r, R] &= A''' [r, R^4], \\
&\dots\dots\dots \\
[r, R^{\beta-2}] \times [r, R] &= A^{(\beta-2)} [r, R^{\beta-1}],
\end{aligned}$$

откуда мы получаем

$$\begin{aligned}[r, R]^2 &= A' [r, R^2], \\ [r, R]^3 &= A' A'' [r, R^3], \\ [r, R]^4 &= A' A'' A''' [r, R^4],\end{aligned}$$

и т. д.,

и, наконец,

$$[r, R]^\beta = \pm n A' A'' A''' \dots A^{(\beta-2)},$$

где следует брать верхний или нижний знак в зависимости от того, является ли число  $(n-1)/\beta$  четным или нечетным.

Отсюда, следовательно, вытекает, что после того, как найдено значение  $[r, R]$ , остальные функции

$$[r, R^2] = \frac{[r, R]^2}{A'}, \quad [r, R^3] = \frac{[r, R]^3}{A' A''}, \dots$$

могут быть здесь определены намного легче, чем в тех случаях, когда  $\alpha$  не равно 1, на что мы уже указывали в «Арифметических исследованиях» (п. 360, III). Эти операции могут быть упрощены еще более детальным рассмотрением природы функций  $A', A'', \dots$

## 15

В п. 9 мы показали, что значение функции  $[r, R]$  может быть приведено к виду  $\sqrt[n]{n}(\cos f + i \sin f)$ , и таким же образом могут быть приведены к подобному же виду и функции  $[r, R^2]$ ,  $[r, R^3]$ , и т. д. до функции  $[r, R^{\beta-1}]$ . Если мы положим

$$\begin{aligned}[r, R] &= \sqrt[n]{n}(\cos f' + i \sin f'), \\ [r, R^2] &= \sqrt[n]{n}(\cos f'' + i \sin f''), \\ [r, R^3] &= \sqrt[n]{n}(\cos f''' + i \sin f'''), \\ &\text{и т. д.,}\end{aligned}$$

то будут выполняться равенства

$$\begin{aligned}A' &= \sqrt[n]{n}[\cos(2f' - f'') + i \sin(2f' - f'')], \\ A'' &= \sqrt[n]{n}[\cos(f' + f'' - f''') + i \sin(f' + f'' - f''')], \\ A''' &= \sqrt[n]{n}[\cos(f' + f''' - f''') + i \sin(f' + f''' - f''')]\end{aligned}$$

и т. д.

Если представить функции  $A', A'', A''', \dots$  в виде

$$\begin{aligned} A' &= a' (\cos b' + i \sin b'), \\ A'' &= a'' (\cos b'' + i \sin b''), \\ A''' &= a''' (\cos b''' + i \sin b'''), \\ &\text{и т. д.} \end{aligned}$$

причем так, что все числа  $a', a'', a''', \dots$  положительны, то мы получаем, что

$$\begin{aligned} a' - a'' = a''' = \dots = \sqrt[n]{n}, \\ f' = \frac{1}{\beta} (b' + b'' + b''' + \dots + b^{(n-2)}), \end{aligned}$$

если  $(n-1)/\beta$  четно, или

$$f' = \frac{1}{\beta} (180^\circ + b' + b'' + b''' + \dots + b^{(n-2)}),$$

если  $(n-1)/\beta$  нечетно, и, далее,

$$\begin{aligned} [r, R] &= \sqrt[n]{n} (\cos f' + i \sin f'), \\ [r, R^2] &= \sqrt[n]{n} (\cos (2f' - b') + i \sin (2f' - b')), \\ [r, R^3] &= \sqrt[n]{n} (\cos (3f' - b' - b'') + i \sin (3f' - b' - b'')), \\ &\text{и т. д.} \end{aligned}$$

Наконец, согласно формулам п. 8,

$$\begin{aligned} \left(\frac{n-1}{\beta}, 1\right) &= -\frac{1}{\beta} + \frac{\sqrt[n]{n}}{\beta} \{ \cos f' + \cos (2f' - b') + \cos (3f' - b' - b'') + \\ &+ \dots + \cos ((\beta-1)f' - b' - b'' - b''' - \dots - b^{(\beta-2)}) \} + \\ &+ \frac{i\sqrt[n]{n}}{\beta} \{ \sin f' + \sin (2f' - b') + \sin (3f' - b' - b'') + \dots + \\ &+ \sin ((\beta-1)f' - b' - b'' - b''' - \dots - b^{(\beta-2)}) \}, \end{aligned}$$

и точно так же получаются значения функций  $\left(\frac{n-1}{\beta}, g\right), \left(\frac{n-1}{\beta}, g^2\right), \left(\frac{n-1}{\beta}, g^3\right), \dots$ , если в этой формуле вместо  $f'$  подставлять соответственно значения  $f' - \frac{360^\circ k}{\beta}, f' - 2 \cdot \frac{360^\circ k}{\beta}, f' - 3 \cdot \frac{360^\circ k}{\beta}, \dots$ , где  $R = \cos \frac{360^\circ k}{\beta} + i \sin \frac{360^\circ k}{\beta}$ .



Еще одно упрощение получается на основании следующего замечания. Так как, согласно п. 14, имеет место

$$\pm [r, R] \times [r, R^{\beta-1}] = [r, R^2] \times [r, R^{\beta-2}] = \pm [r, R^3] [r, R^{\beta-3}] = \dots = n,$$

где (в первом, третьем и т. д. произведениях) нужно брать верхние или нижние знаки в зависимости от того, четно или нечетно число  $(n - 1) / \beta$ , то в первом случае должно быть

$$\cos (f' + f^{(\beta-1)}) = \cos (f'' + f^{(\beta-2)}) = \cos (f''' + f^{(\beta-3)}) = \dots = 1,$$

во втором случае

$$-\cos (f' + f^{(\beta-1)}) = \cos (f'' + f^{(\beta-2)}) = -\cos (f''' + f^{(\beta-3)}) = \dots = 1,$$

и в обоих случаях

$$\sin (f' + f^{(\beta-1)}) = \sin (f'' + f^{(\beta-2)}) = \sin (f''' + f^{(\beta-3)}) = \dots = 0.$$

Поэтому можно положить в первом случае

$$f^{(\beta-1)} = -f', \quad f^{(\beta-2)} = -f'', \quad f^{(\beta-3)} = -f''', \dots,$$

во втором случае

$$f^{(\beta-1)} = 180^\circ - f', \quad f^{(\beta-2)} = 180^\circ - f'', \quad f^{(\beta-3)} = 180^\circ - f''', \dots$$

Но из этого следует, что в первом случае

$$b^{(\beta-2)} = b', \quad b^{(\beta-3)} = b'', \quad b^{(\beta-4)} = b''', \dots,$$

$$A^{(\beta-2)} = A', \quad A^{(\beta-3)} = A'', \quad A^{(\beta-4)} = A''', \dots,$$

а во втором случае

$$b^{(\beta-2)} = b' - 180^\circ, \quad b^{(\beta-3)} = b'' + 180^\circ, \quad b^{(\beta-4)} = b''' - 180^\circ, \dots,$$

$$A^{(\beta-2)} = -A', \quad A^{(\beta-3)} = -A'', \quad A^{(\beta-4)} = -A''', \dots,$$

так что общее число функций  $A', A'', A''', \dots$  сводится к половине.

Далее, отсюда следует, что в первом случае

$$f' = \frac{1}{\beta} \left( 2b' + 2b'' + \dots + 2b^{\left(\frac{1}{2}\beta-1\right)} \right),$$

$$\left( \frac{n-1}{\beta}, 1 \right) = -\frac{1}{\beta} + \frac{V\bar{n}}{\beta} \left\{ 2\cos f' + 2\cos (2f' - b') + \right.$$

$$+ 2\cos (3f' - b' - b'') + \dots +$$

$$+ 2\cos \left( \left( \frac{1}{2}\beta - 1 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-2\right)} \right) +$$

$$\left. + \cos \left( \frac{1}{2}\beta f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-1\right)} \right) \right\}$$

(где последний член, очевидно, равен  $\cos 0 = 1$ ), или

$$f' = \frac{1}{\beta} \left( 2b' + 2b'' + \dots + 2b^{\left(\frac{1}{2}\beta-3\right)} + b^{\left(\frac{1}{2}\beta-1\right)} \right),$$

$$\left( \frac{n-1}{\beta}, 1 \right) = -\frac{1}{\beta} + \frac{V\bar{n}}{\beta} \left\{ 2\cos f' + 2\cos (2f' - b') + \right.$$

$$+ 2\cos (3f' - b' - b'') + \dots +$$

$$\left. + 2\cos \left( \frac{1}{2}(\beta - 1)f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-3\right)} \right) \right\},$$

в зависимости от того, четно  $\beta$  или нечетно; во втором случае

$$f' = \frac{1}{\beta} \left( 2b' + 2b'' + \dots + 2b^{\left(\frac{1}{2}\beta-1\right)} \right),$$

$$\left( \frac{n-1}{\beta}, 1 \right) = -\frac{1}{\beta} + \frac{V\bar{n}}{\beta} \left\{ 2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \dots + \right.$$

$$+ 2\cos \left( \left( \frac{1}{2}\beta - 2 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-3\right)} \right) +$$

$$+ \cos \left( \frac{1}{2}\beta f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-1\right)} \right) \Big\} +$$

$$+ i \frac{V\bar{n}}{\beta} \left\{ 2\sin f' + 2\sin (3f' - b' - b'') + \dots + \right.$$

$$\left. + 2\sin \left( \left( \frac{1}{2}\beta - 1 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-2\right)} \right) \right\},$$

ИЛИ

$$\begin{aligned}
f' &= \frac{1}{\beta} \left( 2b' + 2b'' + \dots + 2b^{\left(\frac{1}{2}\beta-1\right)} + 180^\circ \right), \\
\left( \frac{n-1}{\beta}, 1 \right) &= -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta} \left\{ 2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \right. \\
&+ \dots + 2\cos \left( \left( \frac{1}{2}\beta - 1 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-2\right)} \right) \Big\} + \\
&+ i \frac{\sqrt{n}}{\beta} \left\{ 2\sin f' + 2\sin(3f' - b' - b'') + \dots + \right. \\
&+ 2\sin \left( \left( \frac{1}{2}\beta - 2 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-3\right)} \right) + \\
&+ \sin \left( \left( \frac{1}{2}\beta - 1 \right) f' - b' - b'' - \dots - b^{\left(\frac{1}{2}\beta-2\right)} \right) \Big\},
\end{aligned}$$

в зависимости от того, четно или нечетно число  $\beta/2$ . Для остальных периодов из  $(n-1)/\beta$  членов имеет место то же, что мы заметили выше. Итак, мы заключаем из этого вообще, что для определения этих периодов требуется деление полного круга на  $\beta$  частей, от которого рационально зависит построение углов  $b', b'', b''', \dots$ , далее, деление на  $\beta$  частей угла  $b' + b'' + b''' + \dots$ , и, наконец, извлечение квадратного корня  $\sqrt{n}$ . Если теперь положить одновременно  $\beta = \frac{1}{2}(n-1)$ , то указанные периоды будут, очевидно, совпадать с удвоенными косинусами углов  $360^\circ/n, 2 \cdot 360^\circ/n, 3 \cdot 360^\circ/n, \dots, \frac{1}{2}(n-1)360^\circ/n$ , и потому деление круга на  $n$  частей зависит от деления всего круга на  $(n-1)/2$  частей, от деления на  $(n-1)/2$  частей угла, который может быть построен после выполнения первого деления и от корня  $\sqrt{n}$ . Если же нужно найти и синусы углов  $360^\circ/n, \dots$ , то требуется еще одна операция.

Ради большей ясности мы снова используем пример п. 13, где мы нашли

$$\begin{aligned}
A' &= A''' = 2 + 4R + R^3 + 2R^4 = 2R - 2R^2 - R^3, \\
A'' &= 2 + R + 4R^2 + 2R^3 = -R + 2R^2 - 2R^4.
\end{aligned}$$

Если взять за  $R$  значение  $\cos 72^\circ + i \sin 72^\circ$ , то

$$\begin{aligned} A' = A''' &= 2 \cos 72^\circ - 3 \cos 144^\circ + i (2 \sin 72^\circ - \sin 144^\circ), \\ A'' &= -3 \cos 72^\circ + 2 \cos 144^\circ + i (\sin 72^\circ + 2 \sin 144^\circ). \end{aligned}$$

Поэтому углы  $b', b'', \dots$  определяются уравнениями

$$1) \quad \sin b' = \frac{2 \sin 72^\circ - \sin 144^\circ}{\sqrt{11}},$$

$$2) \quad \cos b' = \frac{2 \cos 72^\circ - 3 \cos 144^\circ}{\sqrt{11}},$$

$$3) \quad \operatorname{tg} b' = \frac{2 \sin 72^\circ - \sin 144^\circ}{2 \cos 72^\circ - 3 \cos 144^\circ},$$

$$4) \quad \sin b'' = \frac{\sin 72^\circ + 2 \sin 144^\circ}{\sqrt{11}},$$

$$5) \quad \cos b'' = \frac{-3 \cos 72^\circ + 2 \cos 144^\circ}{\sqrt{11}},$$

$$6) \quad \operatorname{tg} b'' = \frac{\sin 72^\circ + 2 \sin 144^\circ}{-3 \cos 72^\circ + 2 \cos 144^\circ}.$$

Каждое из уравнений 1), 2), 3) достаточно для определения угла  $b'$ , если известен квадрант, в котором его следует брать; этот квадрант следует определять по знакам величин  $2 \sin 72^\circ - \sin 144^\circ$ ,  $2 \cos 72^\circ - 3 \cos 144^\circ$ ; то же самое имеет место для угла  $b''$ .

В нашем случае угол  $b'$  берется между  $0^\circ$  и  $90^\circ$ , а угол  $b''$  — между  $90^\circ$  и  $180^\circ$ . Если числитель и знаменатель уравнения 3) умножить на  $-3 \cos 72^\circ + 2 \cos 144^\circ$ , то оно перейдет в уравнение

$$\operatorname{tg} b' = \frac{2}{31} \{-\sin 72^\circ + 13 \sin 144^\circ\},$$

и точно так же, если числитель и знаменатель уравнения 6) умножить на  $2 \cos 72^\circ - 3 \cos 144^\circ$ , из него получится следующее уравнение:

$$\operatorname{tg} b'' = \frac{2}{31} \{-13 \sin 72^\circ - \sin 144^\circ\}.$$

Отсюда получаются такие численные значения:

$$\operatorname{tg} b' \approx +0,4316226944; \log \operatorname{tg} b' \approx 9,6351042715; b' \approx 23^\circ 20' 46'',04603;$$

$\operatorname{tg} b'' \approx -0,8355819332; \log \operatorname{tg} b'' \approx 9,9219890411 n; b'' \approx 140^\circ 7' 6'', 52441$ , откуда следует, что

$$5f' \approx 186^\circ 48' 38'', 61647, f' \approx 37^\circ 21' 43'', 723294.$$

Поэтому мы получаем:

$$(2, 1) \approx -\frac{1}{5} + \frac{\sqrt{11}}{5} \{2 \cos 37^\circ 21' 43'', 723294 + 2 \cos 51^\circ 22' 41'', 400558\},$$

$$(2, 2) \approx -\frac{1}{5} + \frac{\sqrt{11}}{5} \{2 \cos 325^\circ 21' 43'', 723294 + 2 \cos 267^\circ 22' 41'', 400558\},$$

$$(2, 4) \approx -\frac{1}{5} + \frac{\sqrt{11}}{5} \{2 \cos 253^\circ 21' 43'', 723294 + 2 \cos 123^\circ 22' 41'', 400558\},$$

$$(2, 8) \approx -\frac{1}{5} + \frac{\sqrt{11}}{5} \{2 \cos 181^\circ 21' 43'', 723294 + 2 \cos 339^\circ 22' 41'', 400558\},$$

$$(2, 5) \approx -\frac{1}{5} + \frac{\sqrt{11}}{5} \{2 \cos 109^\circ 21' 43'', 723294 + 2 \cos 195^\circ 22' 41'', 400558\},$$

откуда мы находим, что

$$(2, 1) \approx +1,6825070652 \approx 2 \cos \frac{360^\circ}{11},$$

$$(2, 2) \approx +0,8308299 \approx 2 \cos \frac{720^\circ}{11},$$

$$(2, 4) = 2 \cos \frac{1440^\circ}{11},$$

$$(2, 8) = 2 \cos \frac{2880^\circ}{11},$$

$$(2, 5) = 2 \cos \frac{1800^\circ}{11}.$$

18

*Другой пример* доставляет нам уравнение  $x^{17} - 1 = 0$ , которое мы другим методом разобрали уже в «*Арифметических исследованиях*». Мы полагаем, таким образом,  $n = 17$ ,  $\beta = 8$ ,  $g = 3$ . Тогда числам 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 соответствуют индексы

$$0, 14, 1, 12, 5, 15, 11, 10, 2, 3, 7, 13, 4, 9, 6, 8.$$

Отсюда мы находим

$$\begin{aligned} A' = A'''' &= * + 2R + 2R^2 + * + 3R^4 + 4R^5 + 2R^6 + 2R^7, \\ A'' = A'''' &= 2 + 3R + * + R^3 + R^4 + 3R^5 + 4R^6 + R^7, \\ A''' = A''' &= 3 + 3R + 2R^2 + 3R^3 + * + R^5 + 2R^6 + R^7, \end{aligned}$$

или, так как в этом случае  $R^4 + 1 = 0$ ,

$$\begin{aligned} A' = A'''' &= -3 - 2R - 2R^3, \\ A'' = A'''' &= 1 - 4R^2, \\ A''' = A''' &= 3 + 2R + 2R^3. \end{aligned}$$

Поэтому если положить  $R = \cos 45^\circ + i \sin 45^\circ$ , то

$$A' = A'''' = -3 - 2i\sqrt{2}, \quad A'' = A'''' = 1 - 4i, \quad A''' = A''' = 3 + 2i\sqrt{2}.$$

Таким образом, величины  $b'$ ,  $b''$ ,  $b'''$  находятся из уравнений

$$\begin{aligned} \sin b' &= -\sqrt{\frac{8}{17}}, \quad \sin b'' = -\sqrt{\frac{16}{17}}, \quad \sin b''' = +\sqrt{\frac{8}{17}}, \\ \cos b' &= -\sqrt{\frac{9}{17}}, \quad \cos b'' = +\sqrt{\frac{1}{17}}, \quad \cos b''' = +\sqrt{\frac{9}{17}}, \\ \operatorname{tg} b' &= +\sqrt{\frac{8}{9}}, \quad \operatorname{tg} b'' = -4, \quad \operatorname{tg} b''' = +\sqrt{\frac{8}{9}}; \end{aligned}$$

из этих уравнений получим

$$(2, 1) \approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times$$

$$\times \{2 \cos 137^\circ 39' 57'' + 2 \cos 52^\circ 1' 5'' + 2 \cos 265^\circ 38' 52'' + 1\},$$

$$(2, 3) \approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times$$

$$\times \{2 \cos 92^\circ 39' 57'' + 2 \cos 322^\circ 1' 5'' + 2 \cos 130^\circ 38' 52'' - 1\},$$

$$(2, 9) \approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times$$

$$\times \{2 \cos 47^\circ 39' 57'' + 2 \cos 232^\circ 1' 5'' + 2 \cos 355^\circ 38' 52'' + 1\},$$

$$(2, 10) \approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times$$

$$\times \{2 \cos 2^\circ 39' 57'' + 2 \cos 142^\circ 1' 5'' + 2 \cos 220^\circ 38' 52' - 1\},$$

$$\begin{aligned}
(2, 13) &\approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times \\
&\times \{2 \cos 317^\circ 39' 57'' + 2 \cos 52^\circ 1' 5'' + 2 \cos 85^\circ 38' 52'' + 1\}, \\
(2, 5) &\approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times \\
&\times \{2 \cos 272^\circ 39' 57'' + 2 \cos 322^\circ 1' 5'' + 2 \cos 310^\circ 38' 52'' - 1\}, \\
(2, 15) &\approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times \\
&\times \{2 \cos 227^\circ 39' 57'' + 2 \cos 232^\circ 1' 5'' + 2 \cos 175^\circ 38' 52'' + 1\}, \\
(2, 11) &\approx -\frac{1}{8} + \frac{\sqrt{17}}{8} \times \\
&\times \{2 \cos 182^\circ 39' 57'' + 2 \cos 142^\circ 1' 5'' + 2 \cos 40^\circ 38' 52'' - 1\};
\end{aligned}$$

$$\frac{1}{2} (2, 1) \approx + 0,092268 \approx \cos \frac{4}{17} 360^\circ,$$

$$\frac{1}{2} (2, 3) = \cos \frac{5}{17} 360^\circ,$$

$$\frac{1}{2} (2, 9) = \cos \frac{2}{17} 360^\circ,$$

$$\frac{1}{2} (2, 10) = \cos \frac{6}{17} 360^\circ,$$

$$\frac{1}{2} (2, 13) \approx + 0,93247 \approx \cos \frac{1}{17} 360^\circ,$$

$$\frac{1}{2} (2, 5) = \cos \frac{3}{17} 360^\circ,$$

$$\frac{1}{2} (2, 15) = \cos \frac{8}{17} 360^\circ,$$

$$\frac{1}{2} (2, 11) = \cos \frac{7}{17} 360^\circ.$$

\* \* \*

От этих более общих исследований о функциях  $[r, R]$ , которые проливают более яркий свет на вторую, начатую в «Арифметических исследованиях», п. 360, теорию, и развивают ее, мы переходим к более подробному рассмотрению некоторых специальных случаев

(именно, когда для  $\beta$  берутся определенные значения); при этом получаются многие сколь плодотворные, столь и изящные факты, некоторые из которых, правда, уже излагались, однако другим методом, в «Арифметических исследованиях», а другие должны рассматриваться как совершенно новые. Однако развитие замечательной связи между этими исследованиями и высшей арифметикой, которая при этом получает весьма значительное и неожиданное обогащение, мы оставим до другого сочинения, которое скоро будет опубликовано. Во всем дальнейшем исследовании мы будем предполагать, что за  $r$  взят собственный корень уравнения  $x^n - 1 = 0$ , и за  $R$  — собственный корень уравнения  $R^\beta - 1 = 0$ .

## 19

Мы начнем со значения  $\beta = 2$ , когда для  $R$ , следовательно, нужно взять значение  $-1$ . Наша функция  $[r, R]$  будет поэтому равна

$$r - r^g + r^{g^2} - r^{g^3} + \dots - r^{g^{n-2}},$$

и мы имеем

$$[r, R] = -[r^g, R] = +[r^{g^2}, R] = -[r^{g^3}, R] = \dots,$$

и вообще, если  $\lambda$  обозначает любое не делящееся на  $n$  целое число, то

$[r^\lambda, R] = +[r, R]$ , если  $\lambda$  есть квадратичный вычет по модулю  $n$ ;

$[r^\lambda, R] = -[r, R]$ , если  $\lambda$  есть квадратичный невычет по модулю  $n$ .

Далее, если произвольные квадратичные вычеты по модулю  $n$ , содержащиеся среди чисел  $1, 2, 3, \dots, n-1$ , обозначать через  $a$ , и произвольные квадратичные невычеты по модулю  $n$ , заключенные в том же интервале, обозначать через  $b$ , то очевидно, что если не обращать внимания на порядок расположения, то числа

$$1, g^2, g^4, \dots, g^{n-3}$$

будут сравнимы по модулю  $n$  с числами  $a$ , и точно так же числа

$$g, g^3, g^5, \dots, g^{n-2}$$

будут сравнимы с числами  $b$ , так что  $[r, R] = \sum r^a - \sum r^b$ .



Поэтому, если мы положим  $\frac{360^\circ}{n} = \omega$  и  $r = \cos k\omega + i \sin k\omega$ , то будет выполняться равенство

$$[r, R] = \sum \cos ak\omega - \sum \cos bk\omega + i \sum \sin ak\omega - i \sum \sin bk\omega.$$

Но, согласно п. 14, квадрат функции  $[r, R]$  равен  $+n$  или равен  $-n$ , в зависимости от того, имеет ли  $n$  вид  $4z + 1$  или  $4z - 1$ , и потому в первом случае  $[r, R] = \pm \sqrt{n}$ , а во втором случае  $[r, R] = \pm i \sqrt{n}$ ; знаки же перед корнями остаются неопределенными. Отсюда получаются следующие формулы для сумм:

I. Если  $n$  имеет вид  $4z + 1$ , то

$$\sum \cos ak\omega - \sum \cos bk\omega = \pm \sqrt{n},$$

$$\sum \sin ak\omega - \sum \sin bk\omega = 0.$$

II. Если  $n$  имеет вид  $4z - 1$ , то

$$\sum \cos ak\omega - \sum \cos bk\omega = 0,$$

$$\sum \sin ak\omega - \sum \sin bk\omega = \pm \sqrt{n}.$$

Далее, так как совокупность всех чисел  $a, b$ , очевидно, совпадает с числами  $1, 2, 3, \dots, n-1$ , то

$$\sum r^a + \sum r^b = r + r^2 + r^3 + \dots + r^{n-1} = -1,$$

и потому

$$\sum \cos ak\omega + \sum \cos bk\omega = -1,$$

$$\sum \sin ak\omega + \sum \sin bk\omega = 0.$$

Поэтому из предыдущих формул для сумм получаются следующие соотношения.

I. Для первого случая

$$\sum \cos ak\omega = -\frac{1}{2} \pm \frac{1}{2} \sqrt{n},$$

$$\sum \cos bk\omega = -\frac{1}{2} \mp \frac{1}{2} \sqrt{n},$$

$$\sum \sin ak\omega = \sum \sin bk\omega = 0.$$

II. Для второго случая

$$\sum \cos ak\omega = \sum \cos bk\omega = 0,$$

$$\sum \sin ak\omega = \pm \frac{1}{2} \sqrt{n},$$

$$\sum \sin bk\omega = \pm \frac{1}{2} \sqrt{n}.$$

Эти суммирования при помощи метода, не очень отличающегося от настоящего, были произведены уже в «Арифметических исследованиях» п. 356; хотя ни один из этих методов не смог устранить неопределенность знаков корней, нам все же недавно удалось в специальном исследовании восполнить этот пробел; мы доказали, что при  $k = 1$  во всех указанных формулах нужно брать верхние знаки.

---

## ДОКАЗАТЕЛЬСТВО НЕКОТОРЫХ ТЕОРЕМ О ПЕРИОДАХ КЛАССОВ ДВОЙНИЧНЫХ ФОРМ ВТОРОЙ СТЕПЕНИ

**Теорема I.** *Число (собственно примитивных) классов с одним и тем же определителем, которые при возведении в  $P$ -ю степень, где  $P$  является либо простым числом, либо степенью  $p^\pi$  простого числа  $p$ , дают главный класс  $K$ , либо равно 1, либо равно степени того же простого числа  $p$ .*

**Доказательство.** Пусть  $(\Omega)$  — полная группа всех классов, о которых идет речь, и  $n$  — их число. Так как главный класс  $K$  обязательно содержится в  $(\Omega)$ , то теорема очевидна, если туда входит только он один. Если же туда входят и другие классы, то число классов, содержащихся в периоде каждого из них, будет степенью числа  $p$ . Пусть  $A$  один из этих классов и пусть его период  $(\mathfrak{A})$  содержит  $p^\alpha$  классов, которые все будут входить в  $(\Omega)$ . Если теперь классы этого периода  $(\mathfrak{A})$  исчерпывают совокупность  $(\Omega)$ , то мы имеем  $p^\alpha = n$ , и теорема доказана; если же нет, то пусть  $B$  — любой не входящий в  $(\mathfrak{A})$  класс из  $(\Omega)$ ; предположим, что его период продолжен до тех пор, пока не получился класс  $bB$ , который одновременно содержится среди классов периода  $(\mathfrak{A})$ ; это обязательно должно случиться, так как по крайней мере главный класс является общим для этого периода и для периода  $(\mathfrak{A})$ . Если предположить теперь, что  $bB$  является первым классом в периоде класса  $B$ , входящим также и в  $(\mathfrak{A})$ , т. е. что  $b$  по возможности наименьшее, то я утверждаю,

1) что  $b$  является степенью числа  $p$ . Действительно, ясно, что если положить  $b = p^\beta h$ ,  $bB = iA$  и  $hk \equiv 1 \pmod{p^\pi}$  (что возможно),

то будет иметь место  $kbB = p^\beta hkB = p^\beta B = ikA$ , т. е.  $p^\beta B$  также будет находиться среди классов периода  $(\mathfrak{A})$ , откуда следует, что  $h = 1$  и  $b = p^\beta$ ;

2) что если совокупность классов  $K, B, 2B, \dots, (b-1)B$  обозначить через  $(\mathfrak{B})$ , то всевозможные композиции класса из  $(\mathfrak{A})$  с классом из  $(\mathfrak{B})$  дадут  $p^{\alpha+\beta}$  различных классов. Действительно, если предположить, что  $tA + nB = t'A + n'B$  и  $n = n'$ , то обязательно  $t = t'$ ; если же  $n > n'$ , то  $(n - n')B = (t' - t)A$ , что невозможно, если  $n$  не равно  $n'$ ;

3) что эти  $p^{\alpha+\beta}$  различных классов содержатся в  $(\Omega)$ , что очевидно.

Если теперь эти  $p^{\alpha+\beta}$  классов исчерпывают совокупность  $(\Omega)$ , то теорема доказана; если же нет, то выберем другой, не содержащийся среди них класс из  $(\Omega)$ , скажем, класс  $C$ , и продолжим его период до тех пор, пока не получим класса, который уже содержится среди классов, составленных из  $(\mathfrak{A})$  и  $(\mathfrak{B})$ . Посредством рассуждений, подобных предыдущим, показывается, что показатель этого класса должен быть степенью числа  $p (= p^\gamma)$  и что композиция  $p^\gamma$  первых классов периода класса  $C$  с уже найденными  $p^{\alpha+\beta}$  классами дает  $p^{\alpha+\beta+\gamma}$  различных классов, которые все содержатся в  $(\Omega)$ . Если эти классы еще не исчерпывают  $(\Omega)$ , то мы таким же образом рассмотрим четвертый класс  $D$ , и т. д., и ясно, что так как  $(\Omega)$  состоит из конечного числа классов, то эта операция тоже будет конечной, и  $n$  будет равно степени числа  $p$ .

**Теорема II.** Если число всех классов главного рода равно  $a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа, то в этом роде существует  $a^\alpha, b^\beta, c^\gamma, \dots$  классов, которые, будучи возведены соответственно в степень  $a^\alpha, b^\beta, c^\gamma, \dots$  дают главный класс.

**Доказательство.** Если  $A, A', A'', \dots$  — всевозможные классы, которые при возведении в степень  $a^\alpha$  дают главный класс  $K$ , и  $(\mathfrak{A})$  — их совокупность; далее, если  $B, B', B'', \dots, (\mathfrak{B})$ ;  $C, C', C'', \dots, (\mathfrak{C})$  и т. д. имеют аналогичные значения, то я утверждаю, что при композиции всевозможных классов из  $(\mathfrak{A})$ , со всевозможными классами из  $(\mathfrak{B})$ , со всевозможными классами из  $(\mathfrak{C})$  и т. д. получаются различные классы. Действительно, если  $A + B + C + \dots = A' + B' + C' + \dots$ , то, полагая  $A - A' = A'', B - B' = B''$

и т. д., мы имеем

$$A'' + B'' + C'' + \dots = K;$$

возводя в степень  $b^\beta c^\gamma \dots$ , мы получаем  $(b^\beta c^\gamma \dots) A'' = K$ , откуда легко видеть, что  $A'' = K$  и  $A = A'$ , и таким же образом мы получаем  $B = B'$ ,  $C = C'$  и т. д. Пусть совокупность этих классов равна  $(S)$ . Ясно, далее, что все эти классы принадлежат главному роду. Наконец, в главном роде нет ни одного класса, который не содержался бы в  $(S)$ . Пусть...

---

# О СВЯЗИ МЕЖДУ ЧИСЛОМ КЛАССОВ, НА КОТОРЫЕ РАСПАДАЮТСЯ ДВОЙНИЧНЫЕ ФОРМЫ ВТОРОЙ СТЕПЕНИ, И ИХ ОПРЕДЕЛИТЕЛЕМ

## I

### 1

Прошло уже тридцать три года с тех пор, как я открыл принципы замечательной связи, которой посвящено настоящее сочинение; я уже указывал на это в конце «*Арифметических исследований*». Однако другие дела долгое время отвлекали меня от этого исследования, пока недавно я не вернулся к нему и не смог благодаря новым усилиям его расширить. Так как, однако, эта новая часть высшей арифметики выходит за рамки одного сочинения, то это первое сочинение будет посвящено формам с отрицательным определителем; формы же с положительным определителем, которые требуют совершенно своеобразного рассмотрения, должны быть оставлены до другого сочинения.

### 2

Основу всего вопроса образует своеобразное исследование о количестве всех комбинаций целочисленных значений, которые принимают два неопределенных целых числа внутри некоторой предписанной области. Очевидно, что эта задача может быть поставлена также и геометрически, именно: найти количество *комплексных чисел*, изображающихся точками внутри некоторой заданной фигуры.

Свойства фигуры зависят от свойств ограничивающей ее линии, т. е. либо от одного уравнения между координатами  $x, y$  (если границей является одна замкнутая кривая), либо от нескольких таких уравнений (если она состоит из нескольких криволинейных или прямолинейных частей), и от нашего желания будет зависеть, причислять ли к рассматриваемому количеству те целые комплексные числа, для которых соответствующие точки лежат на границе, или исключать их.

При аналитическом представлении этой задачи указанные граничные условия всегда могут быть выражены так, что одна или несколько заданных функций  $P, Q, R, \dots$  от переменных  $x, y$  должны принимать положительные или неотрицательные значения (в зависимости от того, исключается или допускается значение 0).

Так, например, если предписанной фигурой является круг, радиус которого равен  $\sqrt{A}$ , в то время как его центр совпадает с точкой, соответствующей некоторому целому комплексному числу, то аналитическим условием этого является то, что выражение  $A - x^2 - y^2$  неотрицательно, если допускать (что мы все время и будем делать) также и точки, лежащие на самой границе. Если фигурой является треугольник, то должны иметь неотрицательные значения три линейные функции  $ax + by + c, a'x + b'y + c', a''x + b''y + c''$ , и аналогично обстоит дело и в других случаях.

### 3

Точное решение задачи должно, вообще говоря, приводиться так: сначала, исходя из природы условий, одна из переменных, например,  $x$ , должна быть заключена в границы, внутри которых она последовательно пробегает все целые значения, а затем нужно определить, сколько целочисленных значений другой переменной  $y$  соответствует каждому отдельному значению переменной  $x$ ; все эти числа затем нужно сложить. В частных случаях по большей части имеются специальные искусственные приемы для сокращения работы.

Пусть, например, как и выше, фигурой является круг с радиусом  $\sqrt{A}$ , и пусть  $r$  — наибольшее целое число, меньшее чем  $\sqrt{A}$ , или само число  $\sqrt{A}$ , если  $A$  является квадратом. Точно так же,

пусть  $r', r'', r''', \dots, r^{(r)}$  — наибольшие целые числа, меньшие, соответственно, чем  $\sqrt{A-1}, \sqrt{A-4}, \sqrt{A-9}, \dots, \sqrt{A-r^2}$ . Тогда искомое количество равно

$$2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \dots = \\ = 1 + 4r + 4r' + 4r'' + 4r''' + \dots + 4r^{(r)}.$$

Короче, однако, в этом примере использовать следующий метод. Пусть  $q$  — наибольшее целое число, меньшее чем  $\sqrt{A/2}$  (или равное  $\sqrt{A/2}$ , если это число целое), и точно так же пусть  $r^{(q+1)}, r^{(q+2)}, r^{(q+3)}, \dots$  — наибольшие целые числа, меньшие соответственно чем  $\sqrt{A-(q+1)^2}, \sqrt{A-(q+2)^2}, \sqrt{A-(q+3)^2}, \dots$ . Тогда искомое количество равно

$$4q^2 + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \dots + r^{(r)}).$$

По этой формуле получаются следующие значения:

| $A$  |      | $A$   |       | $A$    |        |
|------|------|-------|-------|--------|--------|
| 100  | 317  | 1000  | 3149  | 10000  | 31417  |
| 200  | 633  | 2000  | 6293  | 20000  | 62845  |
| 300  | 949  | 3000  | 9425  | 30000  | 94237  |
| 400  | 1257 | 4000  | 12581 | 40000  | 125629 |
| 500  | 1581 | 5000  | 15705 | 50000  | 157093 |
| 600  | 1885 | 6000  | 18853 | 60000  | 188453 |
| 700  | 2209 | 7000  | 21993 | 70000  | 219901 |
| 800  | 2521 | 8000  | 25137 | 80000  | 251305 |
| 900  | 2821 | 9000  | 28269 | 90000  | 282697 |
| 1000 | 3149 | 10000 | 31417 | 100000 | 314197 |

Для нашей цели не требуется нахождения точного значения; нам нужно только получить выражение, которое дает точное количество с любым приближением, если границы стремятся к бесконеч-



ности. Однако, так как здесь еще возможен некоторый произвол, мы должны прежде всего точнее обрисовать положение вещей.

Итак, мы предположим, что функции  $P, Q, R, \dots$ , кроме переменных  $x, y$ , содержат постоянный элемент  $k$ , так что отдельные функции  $P, Q, R, \dots$  являются однородными функциями трех величин  $x, y, k$ . Таким образом, фигура, определенная уравнениями  $P = 0, Q = 0, R = 0, \dots$  будет так зависеть от  $k$ , что различным значениям  $k$  будут соответствовать подобные и подобно расположенные относительно начала координат фигуры, и соответствующие линейные измерения будут пропорциональны значениям  $k$ , а площади пропорциональны значениям  $k^2$ . Если обозначить теперь количество точек внутри фигуры через  $M$ , а площадь через  $V$ , то при возрастании  $k$  должны, очевидно, также возрастать  $M$  и  $V$ ; но если  $k$  будет стремиться к бесконечности, то  $M$  и  $V$  будут сколь угодно близко подходить к отношению равенства, или, если желательна элементарная ясность, сколь бы малая величина  $\lambda$  ни была задана, всегда можно будет указать такую границу, что для каждого значения  $k$ , превосходящего эту границу, отношение  $M/V$  заведомо должно будет лежать между  $1 - \lambda$  и  $1 + \lambda$ . Обычным образом это может быть выражено так: для бесконечно большого значения  $k$  выполняется равенство  $M = V$ .

В нашем примере требуемое условие выполняется, если положить  $k = \sqrt{A}$ ; при этом фигура будет кругом с площадью  $\pi A$ , где  $\pi$  обозначает половину длины окружности с радиусом 1. Приведенные выше числа позволяют ясно убедиться в сходимости.

При желании мы могли бы провести доказательство этой теоремы с полной строгостью, однако мы предпочитаем его в этом месте опустить и перейти к более трудным вещам.

## 5

В этом сочинении граница определяется одним единственным уравнением вида  $ax^2 + 2bxy + cy^2 = A$ , где  $a, b, c$  — целые числа, и  $b^2 - ac$  — отрицательное число, которое мы положим равным  $-D$ . Очевидно, что кривая, определяющая фигуру, будет эллипсом, и легко получается, что квадраты полуосей являются корнями

уравнения  $(ac - b^2) q^2 - A(a + c)q + A^2 = 0$ , т. е. равны

$$A \cdot \frac{a + c \pm \sqrt{4b^2 + (a - c)^2}}{2(ac - b^2)}.$$

Произведение этих корней будет равно  $\frac{A^2}{ac - b^2} = \frac{A^2}{D^2}$ , и потому площадь эллипса равна  $\frac{\pi A}{\sqrt{D}}$

Таким образом, отсюда следует, что число всех комбинаций целочисленных значений переменных  $x, y$ , для которых выражение  $ax^2 + 2bxy + cy^2$  не превосходит значения  $A$ , с ростом  $A$  все более и более приближается к величине  $\pi A / \sqrt{D}$ , и для бесконечно большого  $A$  должно быть положено равным этому значению. Далее, ясно, что в этом отношении безразлично, причислять ли к остальным комбинацию  $x = 0, y = 0$  или исключать ее. Таким образом, искомое количество (в последнем смысле) является ничем иным, как суммой количеств представлений отдельных чисел  $1, 2, 3, \dots, A$  двойничной формой второй степени  $ax^2 + 2bxy + cy^2$ , и так как из этих чисел одни вообще не могут быть представлены этой формой, а другие представляются бóльшим или меньшим числом способов, то величину  $\pi / \sqrt{D}$  следует рассматривать как среднее значение количества представлений неопределенного положительного числа какой-нибудь формой, определитель которой равен  $-D$ .

## 6

Прежде чем переходить к общему изложению дальнейшего, нам представляется целесообразным разобрать некоторые специальные случаи, чтобы легче можно было проникнуть в суть аргументации. Поэтому мы сначала снова возьмем форму  $x^2 + y^2$ , для которой количество представлений неопределенного числа имеет среднее значение  $\pi$ . А количество действительных представлений заданного числа может быть без труда определено при помощи обоснованных в «Арифметических исследованиях» общих принципов. Если мы обозначим через  $f(A)$  количество представлений числа  $A$ , то оно равно 4, если  $A = 1$ , или равно 2, или же равно некоторой степени

числа 2;  $f(A)$  равно 8, если  $A$  является простым числом вида  $4n + 1$  или произведением такого простого числа на степень числа 2;  $f(A) = 0$ , если  $A$  является простым числом вида  $4n + 3$  или делится на такое простое число, но не делится на его квадрат; наконец, вообще, если  $A$  представлено в виде  $2^\alpha S a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа вида  $4n + 1$ , а  $S$  — произведение простых чисел вида  $4n + 3$ , если простые числа такого вида имеются среди сомножителей числа  $A$ , то

$$\begin{aligned} &\text{либо } f(A) = 4(\alpha + 1)(\beta + 1)(\gamma + 1)\dots, \\ &\text{либо } f(A) = 0, \end{aligned}$$

в зависимости от того, является ли число  $S$  квадратом или нет. Таким образом, ясно, что  $f(A)$  полностью определяется теми простыми числами среди 3, 5, 7, 11, 13, ..., которые встречаются среди сомножителей  $A$ , так что вообще нужно положить

$$f(A) = 4(3) \cdot (5) \cdot (7) \cdot (11) \cdot (13) \dots,$$

где (3), (5), (7), ... определяются так. Если  $p$  обозначает простое число, то

во-первых,  $(p) = 1$ , если  $p$  не входит в  $A$ ;

во-вторых,  $(p) = \alpha + 1$ , если  $p$  имеет вид  $4n + 1$  и  $p^\alpha$  есть наивысшая степень, входящая в  $A$ ;

в-третьих,  $(p) = 0$ , если  $p$  имеет вид  $4n + 3$  и показатель наивысшей входящей в  $A$  степени числа  $p$  нечетен; наконец,

в-четвертых,  $(p) = 1$  если  $p$  имеет вид  $4n + 3$ , и показатель наивысшей входящей в  $A$  степени числа  $p$  четен.

Очевидно, что первый случай содержится во втором и четвертом.

Таким образом, члены ряда  $f(1), f(2), f(3), f(4), \dots$  расположены в высшей степени неправильно, хотя по мере увеличения числа все точнее получается среднее значение, равное  $\pi$ . Сумму  $f(1) + f(2) + \dots + f(A)$  мы обозначим через  $F(A)$ .

## 7

Если мы теперь положим вообще  $f(m) + f(3m) = f'(m)$ , то легко видеть, что

$$f'(A) = 4 \cdot (5) \cdot (7) \cdot (11) \cdot (13) \dots,$$

т. е.  $f'(A)$  не зависит от отношения, в котором  $A$  стоит к числу 3, так что неправильность ряда  $f'(1), f'(2), f'(3), f'(4), f'(5), \dots$  будет не только позднее начинаться, но и будет намного меньше. Если мы, далее, положим

$$f'(1) + f'(2) + f'(3) + f'(4) + \dots + f'(m) = F'(m),$$

то

$$F'(3A) = F(3A) + f(3) + f(6) + f(9) + \dots + f(3A) = F(3A) + F(A).$$

Отсюда легко видеть, что если  $A$  возрастает до бесконечности, то нужно положить

$$F'(3A) = 4\pi A,$$

т. е. что среднее значение членов ряда  $f'(1), f'(2), f'(3), f'(4), \dots$  равно  $\frac{4}{3}\pi$ .

Если положить вообще  $-f'(m) + f'(5m) = f''(m)$ , то подобным же образом

$$f''(A) = 4(7) \cdot (11) \cdot (13) \dots,$$

т. е. из нового ряда  $f''(1), f''(2), \dots$  устраняются неправильности, зависящие от отношения  $A$  к числу 5. И если положить

$$f''(1) + f''(2) + f''(3) + \dots + f''(m) = F''(m),$$

то

$$F''(5m) = -F'(m) + F'(5m),$$

откуда следует, что если  $m$  возрастает до бесконечности, то нужно положить

$$F''(5m) = \frac{4}{3}\pi \cdot 4m,$$

или что среднее значение членов ряда равно  $\frac{4}{3} \cdot \frac{4}{5}\pi$ .

Если мы будем продолжать таким же образом и дальше, образуя новые ряды, и исключая последовательно сомножители (7), (11), (13), (17),  $\dots$ , то эти ряды будут все более и более походить на постоянные, а средние значения будут последовательно приобретать

новые сомножители  $8/7, 12/11, 12/13, 16/17, 20/19, \dots$ , знаменателями которых являются простые числа в их натуральном порядке, а числители на единицу больше или меньше знаменателей в зависимости от того, имеют ли эти простые числа вид  $4n - 1$  или  $4n + 1$ . Так как при продолжении этого процесса до бесконечности постоянное значение 4 должно все ближе подходить к среднему значению, мы получаем

$$4 = \pi \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{8}{7} \cdot \frac{12}{11} \cdot \frac{12}{13} \dots \text{ до бесконечности,}$$

или

$$\pi = 4 \cdot \frac{3}{3+1} \cdot \frac{5}{5-1} \cdot \frac{7}{7+1} \cdot \frac{11}{11+1} \cdot \frac{13}{13-1} \dots$$

Если отдельные дроби разложить в бесконечные ряды

$$\frac{3}{3+1} = 1 - \frac{1}{3} + \frac{1}{9} - \frac{1}{27} + \dots,$$

$$\frac{5}{5-1} = 1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \dots,$$

$$\frac{7}{7+1} = 1 - \frac{1}{7} + \frac{1}{49} - \frac{1}{343} + \dots,$$

и т. д.,

то произведение легко преобразуется в

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \dots,$$

и сумма этого ряда, как известно вообще, равна  $\pi/4$ . В действительности Эйлером обратным путем давно было получено отсюда равенство между  $\pi/4$  и бесконечным произведением  $\frac{4}{3} \cdot \frac{4}{5} \cdot \frac{8}{7} \dots$  (*Introd. in analysin inf.*, T. I, Cap. XV, § 285).

Во вторую очередь мы рассмотрим форму  $x^2 + 2y^2$ , для которой количество представлений неопределенного числа будет иметь среднее значение, равное  $\pi/\sqrt{2}$ . Если мы обозначим через  $f(A)$  количество представлений этой формой заданного числа  $A$ , то оно равно 2 для

$A = 1$  или  $A = 2$ , или когда  $A$  является степенью числа 2; далее,  $f(A) = 4$ , если  $A$  является одним из простых чисел, для которых  $-2$  является квадратичным вычетом, т. е. простых чисел вида  $8k + 1$ ,  $8k + 3$ , именно, для  $A = 3, 11, 17, 19, 41, 43, \dots$ ; наконец,  $f(A) = 0$ , если  $A$  является простым числом, для которого  $-2$  есть квадратичный невычет, т. е. простым числом из ряда  $5, 7, 13, 23, 29, 31, \dots$  или простым числом вида  $8k + 5$  или  $8k + 7$ . Вообще, если число  $A$  представлено в виде  $2^\mu S a^\alpha b^\beta c^\gamma \dots$ , где  $a, b, c, \dots$  обозначают различные простые числа вида  $8k + 1, 8k + 3$ , а  $S$  обозначает произведение остальных чисел (вида  $8k + 5, 8k + 7$ ), причем если такие числа содержатся среди сомножителей числа  $A$ , то нужно положить

$$\begin{aligned} &\text{либо } f(A) = 2(\alpha + 1)(\beta + 1)(\gamma + 1) \dots, \\ &\text{либо } f(A) = 0, \end{aligned}$$

в зависимости от того, является ли  $S$  квадратом или нет. Затем, совершенно аналогично тому, как в п. 7, мы переходим от ряда  $f(1), f(2), f(3), f(4), f(5), \dots$ , т. е. ряда  $2, 2, 4, 2, 0, 2, \dots$ , последовательно к рядам, все больше и больше приближающимся к постоянным, средними значениями которых являются по порядку числа  $\pi / \sqrt{2}, 2\pi/3 \sqrt{2}, 2 \cdot 6 \cdot \pi/3 \cdot 5 \cdot \sqrt{2}, 2 \cdot 6 \cdot 8 \cdot \pi/3 \cdot 5 \cdot 7 \sqrt{2}, \dots$ , причем так, что мы приходим к равенству

$$2 = \frac{\pi}{\sqrt{2}} \cdot \frac{2}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{10}{11} \cdot \frac{14}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} \dots,$$

где знаменатели образуют натуральный ряд простых чисел, а числитель на единицу меньше знаменателя, если он имеет вид  $8k + 1$  или  $8k + 3$ , и напротив, на единицу больше знаменателя, если последний имеет вид  $8k + 5$  или  $8k + 7$ .

## II

### 1

Прошло уже тридцать шесть лет с тех пор, как я открыл принципы рассматриваемой в этом сочинении замечательной связи, на что я уже указывал в конце «Арифметических исследований». Однако

другие дела долгое время отвлекали меня от этого исследования, пока я недавно снова не вернулся к нему и не смог благодаря новым усилиям его расширить. Так как, однако, объем этой новой части высшей арифметики выходит за рамки *одного* сочинения, то это первое сочинение будет посвящено формам с отрицательным определителем; формы же с положительным определителем, которые требуют совершенно своеобразного рассмотрения, должны быть оставлены до другого сочинения.

## 2

Для нашей цели мы используем одну теорему, которая сама по себе хотя и является арифметической, но природу которой удобнее и отчетливее можно уяснить, если проводить рассмотрения в геометрической форме.

Если на бесконечной плоскости задана фигура, ограниченная некоторой линией, то площадь этой фигуры может быть приближенно определена, если разбить плоскость на квадраты, и подсчитать количество как тех из них, которые целиком лежат внутри фигуры, так и тех, которые пересекаются границей фигуры, причем площадь, очевидно, будет меньше или больше в зависимости от того, отбрасываются ли последние квадраты, или считаются вместе с первыми. Если же квадраты, лежащие на границе, на основании какого-либо принципа желательнее частью исключать, а частью учитывать, то ошибка будет либо положительной, либо отрицательной, но обязательно меньшей, чем сумма всех квадратов, лежащих на границе. Чем меньшие квадраты брать, тем точнее будет при этом определяться площадь, и такое приближение можно продолжать до бесконечности, т. е. можно брать квадраты настолько малыми, что ошибка будет меньше любой заданной величины. Хотя это кажется очевидным само по себе, мы тем не менее не преминем дать строгое доказательство.

Каждые два квадрата могут иметь либо только одну общую вершину, либо две, либо вообще ни одной; в первом и втором случаях они будут называться соседними, а в третьем случае — разделенными. Очевидно, что квадратов, которые все являются соседними

один с другим, может быть не более четырех, и потому среди любых пяти различных квадратов всегда должно быть по крайней мере два разделенных между собой. Но так как расстояние между двумя точками, лежащими в разделенных квадратах, не меньше стороны квадрата, которую мы обозначим через  $a$ , то очевидно, что если точка, выйдя из какого-нибудь места одного квадрата, пересекает по порядку второй, третий, четвертый квадрат и, наконец, достигает пятого квадрата, то длина пути заведомо будет не меньше чем  $a$ . И так как, если линия далее пересекает другие квадраты, то по аналогичной причине ее части, заключенные между пятым и девятым квадратами, далее, между девятым и тринадцатым квадратами и т. д. — не могут быть меньше чем  $a$ , то мы легко заключаем, что замкнутая линия, которая всего затрагивает  $n$  различных квадратов, заведомо не может быть меньше чем  $(n - 4) a/4$ . Таким образом, наоборот, замкнутая линия, длина которой равна  $l$ , заведомо не может затрагивать более чем  $4 + \frac{4l}{a}$  различных квадратов. Так как их площадь, равная  $4a^2 + 4al$ , может быть сделана меньше любой заданной величины, если  $a$  бесконечно уменьшается, то это же подавно имеет место и для ошибки квадратуры, о которой мы говорили выше.

## 3

Принцип, по которому учитываются или исключаются квадраты, лежащие на границе фигуры, может быть установлен многими различными способами; наиболее простым представляется обращать внимание только на положение центра каждого квадрата, так что квадраты, центры которых лежат внутри фигуры, учитываются, а квадраты, центры которых находятся вне фигуры, исключаются, причем те квадраты, центры которых лежат на самой границе, учитываются или исключаются в зависимости от нашего желания. Вместо центров можно было бы брать также любые другие точки, лежащие в отдельных квадратах аналогичным образом.

Таким образом, дело сводится к тому, что мы представляем себе на плоскости точки, расположенные на одинаковых расстояниях одна от другой и так лежащие на равноудаленных между собой прямых, что получаются квадраты. Тогда, на основании теоремы



предыдущего пункта, мы можем утверждать, что число точек, содержащихся внутри фигуры, умноженное на квадрат расстояния между двумя соседними точками, будет столь мало, сколь мы хотим, отличаться от площади фигуры, если только указанное расстояние взято достаточно малым, или выражаясь обычным образом, что это произведение представляет собой площадь, если расстояние бесконечно мало.

## 4

Кривая, которая представляется уравнением

$$ap^2 + 2bpq + cq^2 = 1$$

в прямоугольных координатах  $p, q$ , является коническим сечением, и притом эллипсом, если величины  $a, c$ , и  $ac - b^2$  положительны; ограниченная этим эллипсом площадь оказывается равной  $\pi / \sqrt{ac - b^2}$ . Значение величины  $ap^2 + 2bpq + cq^2$  вне эллипса всюду больше чем 1, а внутри эллипса меньше чем 1, но нигде не отрицательно.

Представим себе на плоскости, на которой лежит эллипс, систему точек, расположенных так, что они образуют квадраты, стороны которых равны  $\lambda$  и параллельны координатным осям, причем безразлично, совпадает ли начало координат, т. е. центр эллипса, с одной из этих точек или нет. Если количество точек внутри эллипса, считая и те, которые лежат на границе, равно  $m$ , то, согласно теореме предыдущего пункта, число  $\pi / \sqrt{ac - b^2}$  является границей для величины  $m\lambda^2$ , к которой она приближается настолько, насколько нам угодно, если  $\lambda$  бесконечно уменьшается.

Если предположить, что начало координат совпадает с какой-нибудь точкой системы, то если положить  $p = \lambda x$ ,  $q = \lambda y$ , числа  $x$  и  $y$  для отдельных точек системы будут, очевидно, целыми, и, наоборот, каждая комбинация целочисленных значений  $x, y$  будет соответствовать некоторой точке системы. Поэтому число  $m$  является ни чем иным, как количеством всех комбинаций целочисленных значений величин  $x, y$ , для которых  $F$  будет не больше чем  $M$ , если мы для краткости обозначим функцию или форму второй степени  $ax^2 + 2bxy + cy^2$  через  $F$ , а величину  $1/\lambda^2$  — через  $M$ . Опреде-

литель этой формы равен  $b^2 - ac$ , и вместо этого мы будем писать —  $D$ . Поэтому наша теорема теперь будет высказываться следующим образом.

**Теорема I.** *Количество  $t$  всех комбинаций целочисленных значений неизвестных  $x, y$ , для которых значение формы с отрицательным определителем —  $D$  не превосходит границы  $M$ , будет равно  $\pi M / \sqrt{D}$ , причем лишь приближенно, но с бесконечно увеличивающейся точностью приближения, если  $M$  бесконечно возрастает. Вряд ли нужно указывать на то, что бесконечно увеличивающуюся точность приближения надо понимать здесь (как и в дальнейшем) не в том смысле, что сама разность между  $\pi M / \sqrt{D}$  и  $t$  бесконечно уменьшается, а в том, что отношение этих величин все ближе подходит к единице, т. е. что разность  $\frac{\pi M}{t \sqrt{D}} - 1$  бесконечно убывает.*

## 5

Чтобы произвести точный подсчет, можно для отдельных целых значений  $x$ , лежащих между границами  $-\sqrt{\frac{cM}{D}}$  и  $+\sqrt{\frac{cM}{D}}$ , рассматривать по два соответствующих уравнению  $F = M$  значения  $y$ , откуда немедленно получится количество целых чисел, лежащих между ними. Так как это количество одинаково для противоположных значений  $x$ , мы тем самым освобождаемся почти от половины работы. Можно делать и так: подсчитывать значения  $x$ , которые соответствуют отдельным значениям  $y$  между границами  $-\sqrt{\frac{aM}{D}}$  и  $+\sqrt{\frac{aM}{D}}$ . При целесообразном соединении обоих методов работа может быть облегчена еще более, на чем, однако, мы здесь подробнее останавливаться не будем; будет достаточно, если мы добавим кое-что о простейшем случае.

Если формой является  $F = x^2 + y^2$ , т. е. кривая есть окружность, и если  $r, r', r'', r''', \dots, r^{(r)}$  обозначают наибольшие целые числа, которые соответственно меньше чем

$$\sqrt{M}, \sqrt{M-1}, \sqrt{M-4}, \sqrt{M-9}, \dots, \sqrt{M-r^2},$$

или равняются им самим, если среди этих величин содержатся целые числа, то искомое количество  $m$  равно

$$2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \dots + 2(r^{(r)} + 1) = \\ = 1 + 4r + 4r' + 4r'' + 4r''' + \dots + 4r^{(r)}.$$

Однако то же самое мы получим проще, если обозначим через  $q$  наибольшее целое число, меньшее чем  $\sqrt{M/2}$  (или эту самую величину, если она является целым числом), при помощи формулы

$$m = 4q^2 + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \dots + r^{(r)}).$$

Таким образом, получаются следующие количества:

| $M$  | $m$  | $M$   | $m$   | $M$    | $m$    |
|------|------|-------|-------|--------|--------|
| 100  | 317  | 1000  | 3149  | 10000  | 31417  |
| 200  | 633  | 2000  | 6293  | 20000  | 62845  |
| 300  | 949  | 3000  | 9425  | 30000  | 94237  |
| 400  | 1257 | 4000  | 12581 | 40000  | 125629 |
| 500  | 1581 | 5000  | 15705 | 50000  | 157093 |
| 600  | 1885 | 6000  | 18853 | 60000  | 188453 |
| 700  | 2209 | 7000  | 21993 | 70000  | 219901 |
| 800  | 2521 | 8000  | 25137 | 80000  | 251305 |
| 900  | 2821 | 9000  | 28269 | 90000  | 282697 |
| 1000 | 3149 | 10000 | 31417 | 100000 | 314197 |

Теперь мы следующим образом обобщим теорему п. 4.

**Теорема II.** *Если собраны не все комбинации целочисленных значений величин  $x, y$ , для которых  $F$  не превосходит значения  $M$ , а лишь часть из них, именно, те, для которых  $x$  сравнимо по некоторому заданному модулю  $g$  с некоторым заданным числом  $G$ , а  $y$  сравнимо по некоторому заданному модулю  $h$  с некоторым заданным числом  $H$ , то количество  $m'$  этих комбинаций приблизительно будет выражаться значением*

$\pi M / gh \sqrt{D}$ , причем приближение будет беспрестанно становиться все более точным, если  $M$  возрастает до бесконечности.

Действительно, если положить  $x = gx' + G$ ,  $y = hy' + H$ , то  $m'$  будет, очевидно, количеством всех комбинаций целочисленных значений величин  $x'$ ,  $y'$ , для которых

$$ag^2\left(x' + \frac{G}{g}\right)^2 + 2bgh\left(x' + \frac{G}{g}\right)\left(y' + \frac{H}{h}\right) + ch^2\left(y' + \frac{H}{h}\right)^2$$

не превосходит значения  $M$ . Поэтому, если мы представим себе на плоскости систему точек, которые расположены почти так же, как в п. 4, но, кроме того, еще и так, что с некоторой точкой системы совпадает не начало координат, а точка с координатами  $p = \frac{G\lambda}{g}$ ,  $q = \frac{H\lambda}{h}$ , то  $m'$  будет выражать количество точек внутри эллипса, уравнение которого есть

$$ag^2p^2 + 2bghpq + ch^2q^2 = 1,$$

считая также и точки, лежащие на самой границе. И площадь этого эллипса, которая равна  $\frac{\pi}{gh \sqrt{ac - b^2}} = \frac{\pi}{gh \sqrt{D}}$ , будет границей, к которой приближается произведение  $m'\lambda^2 = \frac{m'}{M}$ , когда  $\lambda$  бесконечно убывает или  $M$  бесконечно возрастает.

Ясно, что эта теорема охватывает также и тот случай, когда только одна из двух неизвестных  $x$ ,  $y$  должна изменяться скачками, в то время как значения другой не ограничены никакими условиями. В самом деле, это, очевидно, равносильно тому, чтобы положить  $h$  или  $g$  равным 1.

## 7

До сих пор рассмотрения не зависели от свойств коэффициентов формы  $ax^2 + 2bxy + cy^2$ ; однако, начиная с этого места, мы будем предполагать, что эти коэффициенты являются целыми числами. Таким образом, каждая комбинация целочисленных значений величин  $x$ ,  $y$  будет давать целое значение самой формы, т. е. будет соответствовать представлению этой формой некоторого целого числа.

Отсюда вытекает, что совокупность всех комбинаций целочисленных значений величин  $x, y$ , при которых форма  $F = ax^2 + 2bxy + cy^2$  принимает значения, не превосходящие границы  $M$ , есть ни что иное как совокупность всех представлений целых чисел, которые не превосходят границы  $M$ , или целых чисел до этой границы включительно, если сама она является целым числом. Поэтому, если мы ради краткости обозначим количество различных представлений формой  $F$  определенного целого числа  $n$  через  $F(n)$ , или, чтобы избежать двусмысленности, через  $F_n$ , то обозначенное выше через  $t$  число будет равно  $F_0 + F_1 + F_2 + F_3 + \dots + F_M$ , и первая теорема примет следующий вид.

**Теорема III.** Сумма  $F_0 + F_1 + F_2 + \dots + F_M$  приближенно равна  $\pi M / \sqrt{D}$ , и точность приближения увеличивается беспрестанно, если  $M$  возрастает до бесконечности.

## 8

К третьей теореме, касающейся представлений всех чисел, мы хотим добавить еще одну, которая относится только к нечетным числам. Очевидно, что формой  $F$  не могут представляться нечетные числа, если  $a$  и  $c$  одновременно четны; поэтому исследование ограничивается следующими тремя случаями.

I. Если  $a$  нечетно, а  $c$  четно, то нечетное число будет представляться при нечетном значении  $x$ , в то время как значение  $y$  остается произвольным. Поэтому теорема II, если положить в ней  $g = 2$ ,  $G = 1$ ,  $h = 1$ , показывает, что количество всех комбинаций таких значений  $x, y$ , для которых форма принимает нечетные значения, не превосходящие границы  $M$ , при бесконечно растущем  $M$  с любой степенью точности представляется формулой  $\pi M / 2 \sqrt{D}$ .

II. Если  $a$  четно, а  $c$  нечетно, то для представления нечетного числа нужно, чтобы  $y$  было нечетно, вследствие чего мы, полагая  $g = 1$ ,  $h = 2$ ,  $H = 1$ , приходим к тем же выводам.

III. Если нечетны как  $a$ , так и  $c$ , то для того, чтобы получилось нечетное значение формы, нужно чтобы либо нечетное значение  $x$  комбинировалось с четным значением  $y$ , либо четное значение  $x$

комбинировалось с нечетным значением  $y$ . Количество всех комбинаций как первого, так и второго типа, при которых значение формы не превосходит границы  $M$ , с любой степенью точности выражается формулой  $\pi M / 4 \sqrt{D}$ ; поэтому количество всех комбинаций, которые дают нечетные, не превосходящие границы  $M$ , значения формы, также и здесь с любой степенью точности выражается формулой  $\pi M / 2 \sqrt{D}$ .

Но так как совокупность всех таких комбинаций есть ни что иное как совокупность всех представлений всех чисел  $1, 3, 5, 7, \dots, M$ , если  $M$  — нечетное целое число, или всех чисел  $1, 3, 5, 7, \dots, M-1$ , если  $M$  — четное целое число, то мы получаем следующую теорему.

**Теорема IV. Сумма**

$$F1 + F3 + F5 + F7 + \dots + F(M-1) \\ \text{или } F1 + F3 + F5 + F7 + \dots + FM,$$

в зависимости от того, четно  $M$  или нечетно, с любой степенью точности выражается формулой  $\pi M / 2 \sqrt{D}$ , если  $F$  есть форма, у которой один или оба коэффициента  $a$ ,  $c$  нечетны.

### [III]

Пусть  $C$  — совокупность представителей всех классов собственно примитивных форм для определителя  $-D$ . Обозначим через  $(n)$  количество всех представлений числа  $n$  формами из совокупности  $C$ . Пусть  $p$  — нечетное простое число. Тогда

1.  $(pn) = (n)$ , если  $p$  есть делитель числа  $D$ .
  2.  $(pn) = (n) + (h)$
  3.  $(pn) = -(n) + (h)$
- если  $p$  не делит  $D$  и  $\begin{cases} \text{делит } x^2 + D \\ \text{не делит } x^2 + D, \end{cases}$

где  $n = hr^\mu$ ,  $\mu$  — любое число и  $h$  не делится на  $p$ .

В случае 1 имеет место  $(h) = (ph) = (p^2h) = (p^3h) = \dots$ ;

» » 2 » »  $(ph) = 2(h)$ ,  $(p^2h) = 3(h)$ ,  $(p^3h) = 4(h)$ , ...;

» » 3 » »  $(ph) = 0$ ,  $(p^2h) = (h)$ ,  $(p^3h) = 0$ ,  $(p^4h) = (h)$ , ...;

.....

\* \* \*

Пусть из каждого собственно примитивного класса для определителя  $-D$ , количество которых равно  $\lambda$ , выбрана некоторая форма и совокупность этих форм обозначена через  $L$ .

Обозначим через  $f(A)$  количество всех представлений числа  $A$  формами из  $L$ .

Пусть, далее,  $f(A; p) = f(A / p^\alpha)$ , где  $p^\alpha$  — наивысшая степень простого числа  $p$ , которая входит в  $A$ ; далее,  $f(A; p, q) = f(A / p^\alpha q^\beta)$ , если  $q$  — другое простое число, наивысшая степень которого, входящая в  $A$ , есть  $q^\beta$ ;  $f(A; p, q, r) = f(A / p^\alpha q^\beta r^\gamma)$ , если  $r$  — третье простое число, наивысшей степенью которого, входящей в  $A$ , является  $r^\gamma$ , и т. д.

[IV]

Обозначим через  $(n)$  количество значений  $x$  из совокупности

$$0, 1, 2, 3, 4, \dots, p^n - 1,$$

для которых  $x^2 - D = x^2 - ap^\mu$  делится на  $p^n$ .

1)  $\mu$  нечетно, например,  $= 7$ ,                      2)  $\mu$  четно, например,  $= 6$

|             | $aNp$       | $aRp$        |
|-------------|-------------|--------------|
| $(1) = 1$   | $(1) = 1$   | $(1) = 1$    |
| $(2) = p$   | $(2) = p$   | $(2) = p$    |
| $(3) = p$   | $(3) = p$   | $(3) = p$    |
| $(4) = p^2$ | $(4) = p^2$ | $(4) = p^2$  |
| $(5) = p^2$ | $(5) = p^2$ | $(5) = p^2$  |
| $(6) = p^3$ | $(6) = p^3$ | $(6) = p^3$  |
| $(7) = p^3$ | $(7) = 0$   | $(7) = 2p^3$ |
| $(8) = 0$   | $(8) = 0$   | $(8) = 2p^3$ |
| и т. д.     | и т. д.     | и т. д.      |

| Положим теперь               | Тогда                      |
|------------------------------|----------------------------|
| $(1) - \frac{(2)}{p} = (1)'$ | $f(p) = (1)'$              |
| $(2) - \frac{(3)}{p} = (2)'$ | $f(p^2) = 1 + (2)'$        |
| $(3) - \frac{(4)}{p} = (3)'$ | $f(p^3) = (1)' + (3)'$     |
| $(4) - \frac{(5)}{p} = (4)'$ | $f(p^4) = 1 + (2)' + (4)'$ |
| и т. д.                      | и т. д.                    |

Следовательно, полагая

$$\frac{p-1}{p} \left( 1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \dots \right) = T,$$

мы имеем

$$\frac{p-1}{p} T = 1 + \frac{(1)'}{p} + \frac{(2)'}{p^2} + \frac{(3)'}{p^3} + \frac{(4)'}{p^4} + \dots = 1 + \frac{(1)}{p} = 1 + \frac{1}{p}.$$

Таким образом,  $T = 1$ .

## [V]

Среднее число классов для отрицательного определителя —  $D$  очень близко к

$$\frac{\pi \sqrt{D}}{4 \left( 1 + \frac{1}{27} + \frac{1}{125} + \dots \right)}.$$

Истинное же значение выражается следующей формулой, где ради краткости пишется  $m$  для среднего числа и  $M$  — для истинного;  $p, q$  представляют собой все нечетные простые числа, не входящие в  $D$ , причем  $p$  — делители, а  $q$  — неделители выражения  $x^2 + D$ ;  $r$  обозначает входящие в  $D$  простые числа.



- I.  $M = m \times$  произведение выражений  $\frac{p^3 + p^2}{p^3 - 1} \cdot \frac{q^3 - q^2}{q^3 - 1} \cdot \frac{r^3 - r}{r^3 - 1}$  ;
- II.  $M = \frac{\pi \sqrt{D}}{4} \times$  произведение выражений  $\frac{p + 1}{p} \cdot \frac{q - 1}{q} \cdot \frac{r^2 - 1}{r^2}$  ;
- III. NB.  $M = \frac{2 \sqrt{D}}{\pi} \times$  произведение выражений  $\frac{p}{p - 1} \cdot \frac{q}{q + 1}$  ;
- IV.  $M = \sqrt{\frac{D}{2}} \times$  произведение выражений  $\frac{p + 1}{p - 1} \cdot \frac{q - 1}{q + 1} \cdot \frac{r^2 - 1}{r^2}$  ;
- V.  $M = \frac{2 \sqrt{D}}{\pi} \left\{ 1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \frac{1}{7} \pm \frac{1}{9} \pm \dots \right\}$  .

NB. Формула III непосредственно выводится из сравнения обоих способов для подсчета представляемых чисел до некоторой границы.

## [VI]

**Теорема.** Число классов, на которые распадаются все собственно примитивные двойничные формы, для *отрицательного определителя* —  $D$  равно

$$\frac{\pi}{4} \times \sqrt{D} \times \text{произведение выражений } \frac{p - 1}{p} \cdot \frac{q + 1}{q} \cdot \frac{r^2 - 1}{r^2},$$

где

$p$  обозначает все (нечетные) простые числа, по которым —  $D$  является невычетом,

$q$  обозначает все (нечетные) простые числа, по которым —  $D$  является вычетом,

$r$  обозначает все (нечетные) простые числа, входящие в  $D$ ;

$$= \frac{\frac{\pi}{4} \sqrt{D} \times \text{произведение выражений } \frac{r^2 - 1}{r^2}}{1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \dots},$$

где в знаменателе положительный знак имеют те дроби, знаменатели которых содержатся в форме неделителей выражения  $x^2 + D$ , а отрицательный знак — те дроби, знаменатели которых содержатся в форме делителей; те дроби, знаменатели которых не взаимно просты с  $D$ , вообще отбрасываются;

$$= \frac{2\sqrt{D}\left(1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \dots\right)}{\pi} = \frac{\operatorname{ctg} \theta \pm \operatorname{ctg} 3\theta \pm \operatorname{ctg} 5\theta \pm \dots \pm \operatorname{ctg} n\theta}{N : \sqrt{D}},$$

если положить  $\theta = \frac{\pi}{N}$ ,  $N = \left\{\frac{1}{4}\right\} D$  и за  $n$  брать все взаимно простые с  $D$  числа с определенными выше знаками.

Для положительных определителей число классов

$$= \frac{2\sqrt{D}\left(1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \dots\right)}{\log(T + U\sqrt{D})},$$

где  $T, U$  обозначают наименьшие значения величин  $t, u$ , удовлетворяющие уравнению  $t^2 - Du^2 = 1$ ;

$$= \frac{\log \sin \frac{1}{2} \theta \pm \log \sin \frac{3}{2} \theta \pm \log \sin \frac{5}{2} \theta \pm \dots}{\log(T + U\sqrt{D})}.$$

## [VII]

Для отрицательного определителя  $-p$ , который является простым числом вида  $4n + 1$ , число классов равно  $(\alpha - \beta)$ , где  $\alpha$  обозначает число квадратичных вычетов в первом квадранте

$$1 \cdot 2 \cdot 3 \dots \frac{1}{4}(p-1),$$

$\beta$  — число невычетов.

## [VIII]

$$b \equiv 2m + a - 1 \pmod{8},$$

где  $m$  есть половина числа классов для определителя  $-p$ .

| $p$ | $m$ | $a$ | $b$ | $f$  | $\frac{2m + a - 1 - b}{8}$ | $\alpha$ | $\beta$ |
|-----|-----|-----|-----|------|----------------------------|----------|---------|
| 17  | 2   | + 1 | — 4 | — 4  | +1                         | 3        | 2       |
| 41  | 4   | + 5 | + 4 | + 9  | +1                         | 3        | 4       |
| 73  | 2   | — 3 | — 8 | + 27 | +1                         | 1        | 6       |
| 89  | 6   | + 5 | — 8 | + 34 | +3                         | 9        | 2       |
| 97  | 2   | + 9 | + 4 | + 22 | +1                         | 5        | 6       |
| 113 | 4   | — 7 | + 8 | + 15 | —1                         | 9        | 4       |
| 137 | 4   | —11 | + 4 | + 37 | —1                         | 3        | 8       |
| 193 | 2   | — 7 | +12 | + 81 | —2                         | 11       | 6       |
| 233 | 6   | +13 | + 8 | +144 | +2                         | 15       | 2       |
| 241 | 6   | +15 | + 4 | + 64 | —1                         | 13       | 6       |
| 257 | 8   | + 1 | +16 | + 16 | 0                          | 15       | 4       |
| 281 | 10  | + 5 | —16 | + 53 | +5                         | 9        | 10      |
| 313 | 4   | +13 | —12 | — 25 | +1                         | 5        | 12      |
| 337 | 4   | + 9 | +16 | —148 | 0                          | 7        | 12      |
| 353 | 8   | +17 | + 8 | + 42 | +3                         | 15       | 8       |
| 5   | 1   | + 1 | + 2 | + 2  | 0                          |          |         |
| 13  | 1   | — 3 | — 2 | + 5  | 0                          |          |         |
| 29  | 3   | + 5 | + 2 | + 12 | +1                         |          |         |
| 37  | 1   | + 1 | — 6 | — 6  | +1                         |          |         |
| 53  | 3   | — 7 | — 2 | + 23 | 0                          |          |         |
| 61  | 3   | + 5 | — 6 | + 11 | +2                         |          |         |
| 101 | 7   | + 1 | —10 | — 10 | +3                         |          |         |
| 109 | 3   | — 3 | +10 | + 33 | —1                         |          |         |
| 149 | 7   | — 7 | —10 | + 44 | +2                         |          |         |
| 157 | 3   | —11 | — 6 | — 28 | 0                          |          |         |
| 173 | 7   | +13 | + 2 | + 80 | +3                         |          |         |
| 181 | 5   | + 9 | +10 | — 19 | +1                         |          |         |
| 197 | 5   | + 1 | —14 | — 14 | +3                         |          |         |
| 229 | 5   | —15 | + 2 | —107 | —1                         |          |         |
| 269 | 11  | +13 | +10 | — 82 | +3                         |          |         |
| 277 | 3   | + 9 | +14 | — 60 | 0                          |          |         |
| 293 | 9   | +17 | + 2 | +138 | +4                         |          |         |

| $p$ | $m$ | $a$ | $b$ | $f$  | $\frac{2m + a - 1 - b}{8}$ | $\alpha$ | $\beta$ |
|-----|-----|-----|-----|------|----------------------------|----------|---------|
| 317 | 5   | —11 | +14 | +114 | —2                         |          |         |
| 349 | 7   | + 5 | +18 | —136 | 0                          |          |         |
| 373 | 5   | — 7 | +18 | +104 | —2                         |          |         |
| 389 | 11  | +17 | —10 | —115 | +6                         |          |         |
| 397 | 3   | —19 | — 6 | + 63 | —1                         |          |         |

## [IX]

## Распределение квадратичных вычетов по октантам

$p$  — простое число;  $(r)$  — число квадратичных вычетов по модулю  $p$ , которые лежат между  $(r-1)\frac{p}{8}$  и  $r\frac{p}{8}$ .

П е р в ы й с л у ч а й:  $p = 8n + 1$ .

$2t$  — число классов для определителя  $-p$ ;

$2u$  — число классов для определителя  $-2p$ .

$$(1) = (8) = \frac{1}{4} (2n + t + u),$$

$$(2) = (4) = (5) = (7) = \frac{1}{4} (2n + t - u),$$

$$(3) = (6) = \frac{1}{4} (2n - 3t + u).$$

| $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (3) | $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (3) |
|-----|------|-----|-----|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|
| 17  | 4    | 2   | 2   | 2   | 1   | 0   | 233 | 58   | 6   | 4   | 17  | 15  | 11  |
| 41  | 10   | 4   | 2   | 4   | 3   | 0   | 241 | 60   | 6   | 10  | 19  | 14  | 13  |
| 73  | 18   | 2   | 8   | 7   | 3   | 5   | 257 | 64   | 8   | 8   | 20  | 16  | 12  |
| 89  | 22   | 6   | 4   | 8   | 6   | 2   | 281 | 70   | 10  | 4   | 21  | 19  | 11  |
| 97  | 24   | 2   | 10  | 9   | 4   | 7   | 313 | 78   | 4   | 18  | 25  | 16  | 21  |
| 113 | 28   | 4   | 4   | 9   | 7   | 5   | 337 | 84   | 4   | 12  | 25  | 19  | 21  |
| 137 | 34   | 4   | 6   | 11  | 8   | 7   | 353 | 88   | 8   | 12  | 27  | 21  | 19  |
| 193 | 48   | 2   | 10  | 15  | 10  | 13  | 401 | 100  | 10  | 6   | 29  | 26  | 19  |

Второй случай:  $p = 8n + 5$ .

$2t$  — число классов для определителя —  $p$ ;

$2u$  — число классов для определителя —  $2p$ .

$$(1) = (3) = (6) = (8) = \frac{1}{4} (2n - t + u),$$

$$(2) = (7) = \frac{1}{4} (2n + 3t - u + 2),$$

$$(4) = (5) = \frac{1}{4} (2n - t - u + 2).$$

| $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (4) | $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (4) |
|-----|------|-----|-----|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|
| 5   | 0    | 1   | 1   | 0   | 1   | 0   | 181 | 44   | 5   | 9   | 12  | 13  | 3   |
| 13  | 2    | 1   | 3   | 1   | 1   | 0   | 197 | 58   | 5   | 5   | 12  | 15  | 10  |
| 29  | 6    | 3   | 1   | 1   | 4   | 1   | 229 | 56   | 5   | 13  | 16  | 15  | 10  |
| 37  | 8    | 1   | 5   | 3   | 2   | 1   | 269 | 66   | 11  | 5   | 15  | 24  | 13  |
| 53  | 12   | 3   | 3   | 3   | 5   | 2   | 277 | 68   | 3   | 11  | 19  | 17  | 14  |
| 61  | 14   | 3   | 5   | 4   | 5   | 2   | 293 | 72   | 9   | 9   | 18  | 23  | 14  |
| 101 | 24   | 7   | 3   | 5   | 11  | 4   | 317 | 78   | 5   | 7   | 20  | 22  | 17  |
| 109 | 26   | 3   | 5   | 7   | 8   | 5   | 349 | 86   | 7   | 13  | 23  | 24  | 17  |
| 149 | 36   | 7   | 3   | 8   | 14  | 7   | 373 | 92   | 5   | 13  | 25  | 24  | 19  |
| 157 | 38   | 3   | 13  | 12  | 9   | 6   | 389 | 96   | 11  | 7   | 23  | 31  | 20  |
| 173 | 42   | 7   | 5   | 10  | 15  | 8   | 397 | 98   | 3   | 21  | 29  | 22  | 19  |

Третий случай:  $p = 8n + 3$ .

$t$  — число классов для определителя —  $p$ ,

$2u$  — число классов для определителя —  $2p$ .

$$(1) = (4) = (7) = \frac{1}{4} (2n + t - u),$$

$$(2) = (5) = (8) = \frac{1}{4} (2n - t + u),$$

$$(3) = \frac{1}{4} (2n + t + u + 2),$$

$$(6) = \frac{1}{4} (2n - t - u + 2),$$

| $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (3) | (6) | $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (3) | (6) |
|-----|------|-----|-----|-----|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|-----|
| 3   | 0    | 1   | 1   | 0   | 0   | 1   | 0   | 163 | 40   | 3   | 11  | 8   | 12  | 14  | 7   |
| 11  | 2    | 3   | 1   | 1   | 0   | 2   | 0   | 179 | 44   | 15  | 3   | 14  | 8   | 16  | 7   |
| 19  | 4    | 3   | 3   | 1   | 1   | 3   | 0   | 211 | 52   | 9   | 5   | 14  | 12  | 17  | 10  |
| 43  | 10   | 3   | 5   | 2   | 3   | 5   | 1   | 227 | 56   | 15  | 7   | 16  | 12  | 20  | 9   |
| 59  | 14   | 9   | 3   | 5   | 2   | 7   | 1   | 251 | 62   | 21  | 7   | 19  | 12  | 23  | 9   |
| 67  | 16   | 3   | 7   | 3   | 5   | 7   | 2   | 283 | 70   | 9   | 15  | 16  | 19  | 24  | 12  |
| 83  | 20   | 9   | 5   | 6   | 4   | 9   | 2   | 307 | 76   | 9   | 17  | 17  | 21  | 26  | 13  |
| 107 | 26   | 9   | 3   | 8   | 5   | 10  | 4   | 331 | 82   | 9   | 11  | 20  | 21  | 26  | 16  |
| 131 | 32   | 15  | 3   | 11  | 5   | 13  | 4   | 347 | 86   | 15  | 5   | 24  | 19  | 27  | 17  |
| 139 | 34   | 9   | 7   | 9   | 8   | 13  | 5   | 379 | 94   | 9   | 11  | 23  | 24  | 29  | 19  |

Четвертый случай:  $p = 8n + 7$ .

$t$  — число классов для определителя —  $p$ ;

$2u$  — число классов для определителя —  $2p$ .

$$(1) = \frac{1}{4} (2n + 2t - u),$$

$$(2) = (3) = (5) = \frac{1}{4} (2n + u + 2),$$

$$(4) = (6) = (7) = \frac{1}{4} (2n - u + 2),$$

$$(8) = \frac{1}{4} (2n - 2t + u).$$

| $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (4) | (8) | $p$ | $2n$ | $t$ | $u$ | (1) | (2) | (4) | (8) |
|-----|------|-----|-----|-----|-----|-----|-----|-----|------|-----|-----|-----|-----|-----|-----|
| 7   | 0    | 1   | 2   | 0   | 1   | 0   | 0   | 191 | 46   | 13  | 4   | 17  | 13  | 11  | 6   |
| 23  | 4    | 3   | 2   | 2   | 2   | 1   | 0   | 199 | 48   | 9   | 10  | 14  | 15  | 10  | 10  |
| 31  | 6    | 3   | 4   | 2   | 3   | 1   | 1   | 223 | 54   | 7   | 16  | 13  | 18  | 10  | 14  |
| 47  | 10   | 5   | 4   | 4   | 4   | 2   | 1   | 239 | 58   | 15  | 4   | 21  | 16  | 14  | 8   |
| 71  | 16   | 7   | 2   | 7   | 5   | 4   | 1   | 263 | 64   | 13  | 6   | 21  | 18  | 15  | 11  |
| 79  | 18   | 5   | 4   | 6   | 6   | 4   | 3   | 271 | 66   | 11  | 12  | 19  | 20  | 14  | 14  |
| 103 | 24   | 5   | 10  | 6   | 9   | 4   | 6   | 311 | 76   | 19  | 6   | 27  | 21  | 18  | 11  |
| 127 | 30   | 5   | 8   | 8   | 10  | 6   | 7   | 359 | 88   | 19  | 6   | 30  | 24  | 21  | 14  |
| 151 | 36   | 7   | 6   | 11  | 11  | 8   | 7   | 367 | 90   | 9   | 20  | 22  | 28  | 18  | 23  |
| 167 | 40   | 11  | 6   | 14  | 12  | 9   | 6   | 383 | 94   | 17  | 12  | 29  | 27  | 21  | 18  |

[X]

Распределение квадратичных вычетов по двенадцатым частям.

$p$  — простое число;  $(r)$  — число квадратичных вычетов по модулю  $p$ , которые лежат между  $\frac{r-1}{12} p$  и  $\frac{r}{12} p$ .

Первый случай:  $p = 24n + 1$ .

$2t$  — число классов для определителя  $-p$ .

$4u$  — число классов для определителя  $-3p$ .

$$(1) = (12) = \frac{1}{6} (6n + 3t + 2u),$$

$$(2) = (4) = (6) = (7) = (9) = (11) = \frac{1}{6} (6n - 3t + 2u),$$

$$(3) = (5) = (8) = (10) = \frac{1}{6} (6n + 3t - 4u).$$

| $p$ | $n$ | $t$ | $u$ | (1) | (2) | (3) |
|-----|-----|-----|-----|-----|-----|-----|
| 73  | 3   | 2   | 3   | 5   | 3   | 2   |
| 97  | 4   | 2   | 3   | 6   | 4   | 3   |
| 193 | 8   | 2   | 6   | 11  | 9   | 5   |
| 241 | 10  | 6   | 3   | 14  | 8   | 11  |

Второй случай:  $p = 24n + 13$ .

$2t$  — число классов для определителя  $-p$ ;

$4u$  — число классов для определителя  $-3p$ .

$$(1) = (3) = (10) = (12) = \frac{1}{2} (2n + 1 + t),$$

$$(2) = (6) = (7) = (11) = \frac{1}{2} (2n + 1 - t),$$

$$(4) = (9) = \frac{1}{2} (2n + 1 - t + 2u),$$

$$(5) = (8) = \frac{1}{2} (2n + 1 + t - 2u).$$

| $p$ | $n$ | $t$ | $u$ | (1) | (2) | (4) | (5) |
|-----|-----|-----|-----|-----|-----|-----|-----|
| 13  | 0   | 1   | 1   | 1   | 0   | 1   | 0   |
| 37  | 1   | 1   | 2   | 2   | 1   | 3   | 0   |
| 61  | 2   | 3   | 2   | 4   | 1   | 3   | 2   |
| 109 | 4   | 3   | 3   | 6   | 3   | 6   | 3   |
| 157 | 6   | 3   | 4   | 8   | 5   | 9   | 4   |
| 181 | 7   | 5   | 3   | 10  | 5   | 8   | 7   |
| 229 | 9   | 5   | 3   | 12  | 7   | 10  | 9   |

Третий случай:  $p = 24n + 5$ .

$2t$  — число классов для определителя  $-p$ ;

$2u$  — число классов для определителя  $-3p$ .

$$(1) = (2) = (6) = (7) = (11) = (12) = n,$$

$$(3) = (10) = \frac{1}{2}(2n + 1 + t),$$

$$(4) = (9) = \frac{1}{2}(2n - t + u).$$

$$(5) = (8) = \frac{1}{2}(2n + 1 - u).$$

| $p$ | $n$ | $t$ | $u$ | (1) | (3) | (4) | (5) |
|-----|-----|-----|-----|-----|-----|-----|-----|
| 5   | 0   | 1   | 1   | 0   | 1   | 0   | 0   |
| 29  | 1   | 3   | 3   | 1   | 3   | 1   | 0   |
| 53  | 2   | 3   | 5   | 2   | 4   | 3   | 0   |
| 101 | 4   | 7   | 5   | 4   | 8   | 3   | 2   |
| 149 | 6   | 7   | 7   | 6   | 10  | 6   | 3   |
| 173 | 7   | 7   | 9   | 7   | 11  | 8   | 3   |
| 197 | 8   | 5   | 11  | 8   | 11  | 11  | 3   |
| 269 | 11  | 11  | 7   | 11  | 17  | 9   | 8   |



Четвертый случай:  $p = 24n + 17$ .

$2t$  — число классов для определителя  $-p$ ;

$2u$  — число классов для определителя  $-3p$ .

$(1) = (2) = (6) = (7) = (11) = (12) = \frac{1}{6} (6n + 3 + u);$

$(3) = (10) = \frac{1}{6} (6n + 6 + 3t - 2u),$

$(4) = (9) = \frac{1}{6} (6n + 3 - 3t + u),$

$(5) = (8) = \frac{1}{6} (6n + 6 - 2u).$

| $p$ | $n$ | $t$ | $u$ | (1) | (3) | (4) | (5) |
|-----|-----|-----|-----|-----|-----|-----|-----|
| 17  | 0   | 2   | 3   | 1   | 1   | 0   | 0   |
| 41  | 1   | 4   | 3   | 2   | 3   | 0   | 1   |
| 89  | 3   | 6   | 3   | 4   | 6   | 1   | 3   |
| 113 | 4   | 4   | 9   | 6   | 4   | 4   | 2   |
| 137 | 5   | 4   | 9   | 7   | 5   | 5   | 3   |
| 233 | 9   | 6   | 15  | 12  | 8   | 9   | 5   |
| 257 | 10  | 8   | 9   | 12  | 12  | 8   | 8   |



---

## БОЛЕЕ ПОДРОБНОЕ РАССМОТРЕНИЕ НЕКОТОРЫХ ВОПРОСОВ, ОТНОСЯЩИХСЯ К ДЕЛЕНИЮ КРУГА

367

То, что мы изложили в последней части седьмого раздела, начиная с п. 355, представляет собой убедительный пример как большой плодотворности учения о делении круга, так и замечательной связи этой дисциплины с различными арифметическими исследованиями. Однако, будучи слишком ограничены и объемом работы и временем, мы смогли там лишь слегка коснуться этого круга вопросов, который вознаграждает наши усилия тем более богатыми результатами, чем дальше мы в нем продвигаемся. Поэтому мы намерены снова вернуться здесь к некоторым начатым там исследованиям и разобрать их более подробно, причем читатель несомненно не очень удивится, увидев, что решение многих проблем, издавна рассматривавшихся всеми по-разному, базируется на этом фундаменте.

368

Плодотворнейшие возможности открывает исследование, начатое в п. 356, где мы, после того как совокупность корней уравнения  $x^n - 1 = 0$  (за исключением единицы) была разбита на два класса, показали, как находить сумму корней в каждом из классов, при-

чем эти суммы оказались равными  $-\frac{1}{2} + \frac{1}{2}\sqrt{n}$  и  $-\frac{1}{2} - \frac{1}{2}\sqrt{n}$  для случая, когда  $n$  имеет вид  $4m + 1$ , и равными  $-\frac{1}{2} + \frac{1}{2}\sqrt{-n}$  и  $-\frac{1}{2} - \frac{1}{2}\sqrt{-n}$  для случая, когда  $n$  имеет вид  $4m + 3$ . Однако мы там не только ограничились случаем, когда  $n$  является простым числом, но, что еще более существенно, оставили также неопределенными знаки корней, не подкрепив их определение, лишь кратко набросанное, строгим доказательством. Поэтому мы прежде всего должны восполнить этот пробел.

## 369

Итак, пусть теперь  $n$  — любое целое положительное число,  $R$  — такой корень уравнения  $x^n - 1 = 0$ , что никакая его степень, более низкая, чем  $n$ -я, не равна единице (ср. п. 359, II), и пусть, как и в седьмом разделе, через  $[\lambda]$  обозначена степень  $R^\lambda$ , так что  $[0] = 1, [1], [2], [3], \dots, [n-1]$  представляют все корни уравнения  $x^n - 1 = 0$ . Далее, обозначим сумму

$$[0] + [1] + [4] + [9] + \dots + [(n-1)^2] \text{ через } \sum [\mathfrak{A}],$$

и более общо

$$[0] + [\lambda] + [4\lambda] + [9\lambda] + \dots + [\lambda(n-1)^2] \text{ — через } \sum [\mathfrak{A}\lambda],$$

так что  $\mathfrak{A}$  пробегает квадраты чисел  $0, 1, 2, 3, \dots, n-1$ . Таким образом, очевидно, что так же, как вообще  $[\lambda] = [\mu]$ , если  $\lambda, \mu$  являются некоторыми (положительными или отрицательными) целыми числами, сравнимыми по модулю  $n$ , так и  $\sum [\mathfrak{A}\lambda] = \sum [\mathfrak{A}\mu]$ , если  $\lambda \equiv \mu$ . После этих приготовлений мы имеем следующую задачу.

## 370

**Задача.** Определить произведение сумм  $\sum [\mathfrak{A}]$  и  $\sum [-\mathfrak{A}]$ .

**Решение.** Так как  $n^2 \equiv 0, (n+1)^2 \equiv 1, (n+2)^2 \equiv 4, \dots \pmod{n}$ , то легко получается, что

$$\begin{aligned}\sum [\mathfrak{A}] &= [1] + [4] + [9] + [16] + \dots + [n^2] = \\ &= [4] + [9] + [16] + [25] + \dots + [(n+1)^2] = \\ &= [9] + [16] + [25] + [36] + \dots + [(n+2)^2] = \\ &\quad \dots \dots \dots\end{aligned}$$

или вообще

$$= [k^2] + [(k+1)^2] + [(k+2)^2] + [(k+3)^2] + \dots + [(n+k-1)^2].$$

Отсюда

$$\begin{aligned}[-k^2] \times \sum [\mathfrak{A}] &= \\ &= [0] + [2k+1] + [4k+4] + [6k+9] + \dots + [(n-1)^2 + 2(n-1)k].\end{aligned}$$

Поэтому  $\sum [-\mathfrak{A}] \times \sum [\mathfrak{A}]$  преобразуются в

$$\begin{aligned}&[0] + [1] + [4] + [9] + \dots + [(n-1)^2] + \\ &+ [0] + [3] + [8] + [15] + \dots + [n^2 - 1] + \\ &+ [0] + [5] + [12] + [21] + \dots + [n^2 + 2n - 3] + \\ &+ [0] + [7] + [16] + [27] + \dots + [n^2 + 4n - 5] + \\ &\quad \dots \dots \dots + [0] + [2n-1] + [4n] + [6n+3] + \dots + [3n^2 - 6n + 3].\end{aligned}$$

Если сложить отдельные вертикальные ряды, мы получим

$$\begin{aligned}n[0] + [1] \frac{1-[2n]}{1-[2]} + [4] \frac{1-[4n]}{1-[4]} + [9] \frac{1-[6n]}{1-[6]} + \dots + \\ + [(n-1)^2] \frac{1-[2n^2-2n]}{1-[2n-2]},\end{aligned}$$

и если  $n$  нечетно, то в этом выражении исчезнут все части, кроме первой, так как будут равны нулю все числители  $1-[2n]$ ,  $1-[4n]$ ,  $1-[6n]$ , ..., и напротив, не равны нулю все знаменатели  $1-[2]$ ,  $1-[4]$ ,  $1-[6]$ ,  $1-[8]$ , ...,  $1-[2n-2]$ . Если же  $n$  — четное число, то будет равен нулю и один из знаменателей, именно,  $1-[n]$ , которому соответствует член  $\left[\frac{1}{4} n^2\right] \frac{1-[n^2]}{1-[n]}$ ; но сумма частей, из которых этот член получился, будет равна  $n \left[\frac{1}{4} n^2\right]$ . Здесь снова нужно различать два случая. Если  $n$  делится на 4, то  $\frac{1}{4} n^2 \equiv 0 \pmod{n}$ , и потому  $\left[\frac{1}{4} n^2\right] = 1$ ; если же  $n$  четно, но не

делится на 4, то  $\frac{1}{4}n^2 \equiv \frac{1}{2}n \pmod{n}$ , и потому обязательно  $\left[\frac{1}{4}n^2\right] = -1$ . Из этого, наконец, следует:

- 1) для нечетного значения  $n$  искомое произведение равно  $n$ ;
- 2) для значения  $n$ , делящегося на 4, оно равно  $2n$ ;
- 3) для четного, но не делящегося на 4 значения  $n$  оно равно 0.

## 371

Стоит потрудиться над тем, чтобы подробнее рассмотреть природу суммы  $\sum [\mathfrak{A}]$ .

I. Так как вместо квадратов 0, 1, 4, 9, 16, ... можно подставлять их наименьшие вычеты по модулю  $n$ , то ясно, что если  $M$  пробегает квадратичные вычеты по модулю  $n$  среди чисел от 0 до  $n-1$ , и  $m$  обозначает количество корней сравнения  $x^2 \equiv M \pmod{n}$ , то  $\sum [\mathfrak{A}] = \sum m[M]$ . Как определяется число  $m$ , мы показали в пп. 104 и 105.

II. Если  $n$  есть (нечетное) простое число, то  $m = 1$  для  $M \equiv 0$ , и  $m = 2$  для каждого другого значения  $M$ . Если же  $n$  является степенью нечетного простого числа, например, равно  $p^\nu$ , то  $m = 2$  для каждого значения  $M$ , не делящегося на  $p$ , . . . . .

## 372

Если  $n$  — (нечетное) простое число, то совокупность вычетов  $M$  состоит из нуля, для которого  $m = 1$ , и из  $(n-1)/2$  других чисел, для которых  $m = 2$ . Если  $\mu$  пробегает эти вычеты (за исключением вычета 0), то наш ряд равен  $1 + 2\sum r^\mu$ . Если, далее,  $\nu$  пробегает все остальные числа, меньшие чем  $n$ , количество которых тоже равно  $(n-1)/2$  и которые охватывают все квадратичные невычеты по модулю  $n$ , меньшие чем  $n$ , то очевидно, что

$$1 + \sum r^\mu + \sum r^\nu = 1 + r + r^2 + r^3 + \dots + r^{n-1} = \frac{1-r^n}{1-r} = 0.$$

Поэтому, если положить сумму нашего ряда, т. е.  $1 + 2\sum r^\mu$ , равной  $A$ , то  $1 + 2\sum r^\nu = -A$ , и  $\sum r^\mu - \sum r^\nu = A$ .

Согласно п. 356, мы имеем тем самым  $A = \pm \sqrt{n}$  или  $\pm \sqrt{-n}$ , в зависимости от того,  $n \equiv 1$  или  $\equiv 3 \pmod{4}$ . Однако знак этим еще не определяется.

Если в наш ряд, который мы обозначим через II, подставить вместо  $r$  другой подобный же корень уравнения  $x^n - 1 = 0$ , скажем,  $r' = r^\lambda$ , то получающийся ряд будет обозначаться через II'.

### 373

Если  $n$  является квадратом или более высокой степенью простого числа, скажем,  $= p^\pi$ , то одни из вычетов  $M$  будут являться числами, не делящимися на  $p$ , другие будут делиться на  $p^2$ , но не будут делиться на более высокую степень числа  $p$ , третьи будут делиться на  $p^4$ , но не будут делиться на  $p^5$  и т. д., до тех вычетов, которые делятся на  $p^{\pi-2}$ , но не делятся на  $p^{\pi-1}$  или делятся на  $p^{\pi-1}$ , но не делятся на  $p^\pi$ , в зависимости от того, четно  $\pi$  или нечетно; наконец, имеется еще вычет 0, который является единственным, делящимся на  $p^\pi$  (ср. п. 102). Если теперь  $\mu$  пробегает квадратичные вычеты числа  $p$ , меньшие чем  $p$  (за исключением нуля), количество которых равно  $\frac{1}{2}(p-1)$ , то указанные различные типы вычетов будут представляться следующим образом. Первые, которые не делятся на  $p$ , будут представляться в виде  $\mu + kp$ , где в качестве  $k$  нужно брать все целые числа от 0 до  $p^{\pi-1}-1$ , так что количество всех вычетов такого вида равно  $\frac{1}{2}(p-1)p^{\pi-1}$ ; для каждого из них  $m=2$ . Сумма всех членов в II, соответствующих этим вычетам, равна

$$2 \sum r^{\mu+kp} = 2 \sum r^{\mu} \cdot \sum r^{kp} = 2 \sum r^{\mu} \cdot \frac{r^{p^\pi} - 1}{r^p - 1} = 0.$$

Второй класс вычетов представляется в виде  $\mu p^2 + kp^3$ , где в качестве  $k$  нужно брать все целые числа от 0 до  $p^{\pi-3}-1$ , так что количество всех вычетов такого вида равно  $\frac{1}{2}(p-1)p^{\pi-3}$ ; для каждого из них будет  $m=2p$ . Сумма получающихся отсюда членов в

ряде II будет равна

$$2p \sum r^{\mu p^2 + kp^3} = 2p \sum r^{\mu p^2} \cdot \sum r^{kp^3} = 2p \sum r^{\mu p^2} \cdot \frac{r^{p^3} - 1}{r^{p^3} - 1} = 0,$$

если  $\pi > 3$ . Аналогичным образом третий, четвертый и т. д. классы представляются соответственно в виде  $\mu p^4 + kp^5$ ,  $\mu p^6 + kp^7, \dots$ , где за  $k$  нужно брать все целые числа от 0 до (соответственно)  $p^{\pi-5} - 1$ ,  $p^{\pi-7} - 1, \dots$ ; для них  $m = 2p^2$ ,  $m = 2p^3, \dots$ . И в ряде II обращаются в нуль суммы членов, получающихся из третьего, четвертого и т. д. классов, если соответственно  $\pi > 5$ ,  $\pi > 7, \dots$

Отсюда для случая, когда  $\pi$  четно, следует, что в II остаются только те члены, которые соответствуют вычету 0 и равны 1. Но для них  $m = p^{\pi/2}$ , так что сумма всех членов в II равна  $p^{\pi/2}$ .

---

# ПРИЛОЖЕНИЯ





## О Т Р Е Д А К Ц И И

Почти все работы великого математика Гаусса были опубликованы им на латинском языке. В настоящем издании впервые публикуются в русском переводе все работы Гаусса по теории чисел. Перевод выполнен кандидатом физико-математических наук В. Б. Демьяновым в основном с прекрасного немецкого перевода Мазера (H. Maser; изд. Springer, 1889), но некоторые места перевода были, кроме того, сверены членом-корреспондентом АН СССР Б. Н. Делоне с подлинным латинским текстом. В «Приложениях» даны статья академика И. М. Виноградова «Карл Фридрих Гаусс» и статья-комментарий члена-корреспондента АН СССР Б. Н. Делоне «Работы Гаусса по теории чисел», облегчающая чтение текста работ Гаусса.

Академик И. М. Виноградов

## КАРЛ ФРИДРИХ ГАУСС \*

Великому немецкому математику Карлу Фридриху Гауссу принадлежат глубокие и основополагающие исследования почти во всех основных областях математики: в теории чисел, в геометрии, в теории вероятностей, в анализе, в алгебре, а также важные исследования в астрономии, в геодезии, в механике и в теории магнетизма.

Математический гений Гаусса развивался на исследованиях по теории целых чисел, завершившихся опубликованием в 1801 г. его знаменитой книги «*Disquisitiones arithmeticae*». В дальнейшем Гаусс возвращался к этим исследованиям и дал в области теории чисел еще две важные работы.

В «*Disquisitiones arithmeticae*» Гаусс изложил все существенное, что было известно в теории чисел до него, но часто исходя из более общих и более принципиальных соображений. Кроме того, «*Disquisitiones arithmeticae*» в четвертом, пятом и седьмом своих разделах заключают три крупнейших открытия самого Гаусса: доказательство квадратичного закона взаимности, композицию классов и родов квадратичных форм и теорию деления круга.

Квадратичный закон взаимности является центральной теоремой теории квадратичных вычетов, доказательство которой долго и

---

\* Речь акад. И. М. Виноградова на торжественном заседании, организованном Всесоюзным обществом культурной связи с заграницей и Отделением физико-математических наук АН СССР 23 февраля 1955 г., по случаю столетия со дня смерти К. Ф. Гаусса.

безуспешно пытались получить крупнейшие математики того времени. Исследования Гаусса по квадратичному и, позже, по биквадратичному закону взаимности послужили исходным пунктом длинного ряда работ, приведших в конечном итоге к отысканию общего закона взаимности, представляющего собой одну из важных теорем теории алгебраических чисел.

Исследования Гаусса по композиции классов и родов квадратичных форм явились важным первым этапом в труднейшем вопросе о построении арифметики полей алгебраических чисел. Исследования Гаусса по целым комплексным числам, опубликованные позже (в 1832 г.), дали пример поля алгебраических чисел, отличного от рационального, в котором действуют законы обычной арифметики. Продолжение обоих этих исследований привело во второй половине XIX столетия к построению общей теории алгебраических чисел, которая является в настоящее время одним из основных методов теории чисел.

Теория деления круга, занимающая последний, седьмой раздел «*Disquisitiones arithmeticae*», содержит подробное рассмотрение двучленного уравнения  $x^n = 1$ , в котором, применяя методы теории чисел, Гаусс сводит решение этого уравнения на цепь уравнений низших степеней. Это исследование представляет собой частный, но вполне заверченный случай теории, построенной впоследствии Галуа, которая является одной из основных теорий алгебры. Теория деления круга дала замечательный чисто геометрический результат. К тем правильным многоугольникам, которые умели строить при помощи циркуля и линейки древние математики, Гаусс прибавил еще правильный семнадцатиугольник. Более того, он нашел вообще все те правильные многоугольники, которые можно построить при помощи циркуля и линейки. Теорема о правильном семнадцатиугольнике была опубликована Гауссом без доказательства, когда он был еще 19-летним студентом, и создала ему первую известность.

В связи с теорией деления круга Гаусс рассмотрел в 1811 г. особые тригонометрические суммы, называемые теперь суммами Гаусса. Дальнейшее обобщение этого исследования привело впоследствии к рассмотрению более общих тригонометрических сумм, которые являются сейчас одним из самых сильных средств аналитической

теории чисел и способствовали доказательству важных теорем, касающихся обыкновенных целых чисел.

О работах Гаусса, не относящихся к области теории чисел, я скажу уже более кратко. Подобно тому, как это было у Архимеда, Ньютона, Эйлера и, впоследствии, у Чебышева, большинство из этих работ было вызвано задачами, которые ставили естествознание и практическая деятельность. Так, работы по геодезической съемке, которые были поручены Гауссу, привели его к исследованиям по внутренней геометрии поверхностей. Они были опубликованы в 1828 г. в знаменитом мемуаре «*Disquisitiones generales circa superficies curvas*». В этом мемуаре содержится также доказательство важной теоремы Гаусса о неизменяемости кривизны при изгибании поверхностей. Непосредственным обобщением идеи Гаусса о внутренней геометрии поверхностей явилась впоследствии геометрия Римана, послужившая в свою очередь основным аппаратом для общей теории относительности.

Обширные приближенные вычисления, которые приходилось практически производить лично Гауссу при решении задач, относящихся к астрономии и к геодезии, привели его к более глубокой разработке способа наименьших квадратов и к выяснению центрального значения нормальной кривой распределения в вопросах, связанных с теорией вероятностей.

Работы Гаусса по теории магнетизма привели его к важным теоремам теории потенциала.

Размышляя над основными принципиальными вопросами механики, Гаусс пришел к известному своему принципу наименьшего действия.

Еще в самый первый период своей научной деятельности, в связи с необходимостью обнаружить на небе потерянную малую планету Цереру, Гаусс придумал замечательный метод определения орбиты по трем наблюдениям. Успех этого метода, давшего возможность снова найти Цереру, был первым обстоятельством, которое сделало имя Гаусса всемирно известным.

Сделаю несколько общих замечаний об особенностях стиля творчества Гаусса. Все общие математические идеи появлялись у Гаусса в связи с решением совершенно конкретных задач. Но эти задачи

большей частью относились к важным узловым вопросам современной ему математики. В дальнейшем, в руках его продолжателей, идеи Гаусса привели к созданию новых областей математики. В частности, работы Гаусса по теории чисел предопределили развитие теории чисел более чем на столетие; такую же роль сыграли и работы Гаусса по внутренней геометрии поверхностей.

После Гаусса осталось обширное рукописное наследие, которое было опубликовано много позже его смерти. В рукописях Гаусса математики с изумлением нашли целый ряд теорем, данных без доказательства и касающихся самых различных отделов математики: аналитической теории чисел, теории эллиптических и, в частности, модулярных функций, неевклидовой геометрии и т. д. Некоторые из этих теорем были, задолго до обнаружения посмертных рукописей Гаусса, независимо от Гаусса, открыты и опубликованы другими математиками, а многие не были еще известны и послужили стимулом для работ последующих ученых.

Русские математики всегда высоко ценили и глубоко изучали работы Гаусса. Некоторые исследования русских математиков являлись непосредственным продолжением работ Гаусса, например: исследования русских математиков о минимумах определенных и неопределенных квадратичных форм, работы по общей теории алгебраических чисел, а в последнее время — работы по общему закону взаимности и исследования, переносящие гауссову внутреннюю геометрию поверхностей на случай не аналитических поверхностей.

Указанная глубокая связь, которая всегда существовала между немецкими и русскими математиками, должна служить примером того дружеского сотрудничества, к которому мы стремимся во всех областях нашей жизни и которое принесет пользу обоим нашим великим народам.

Б. Н. Делоне

## РАБОТЫ ГАУССА ПО ТЕОРИИ ЧИСЕЛ

### 1. Теория чисел до Гаусса

Важные теоремы о целых числах были доказаны уже в древности. Так, например, в школе Пифагора (V в. до н. э.) были найдены в бесконечном числе такие взаимно простые квадраты целых чисел, сумма которых тоже квадрат  $x^2 + y^2 = z^2$ . В «Началах» Эвклида (III в. до н. э.) мы находим доказательство бесконечности числа простых чисел. В сочинении Диофанта (III в. н. э.) рассмотрены способы решения различных неопределенных уравнений в рациональных числах.

Первый, кто в новое время начал глубокие исследования целых чисел, был Пьер Ферма (1601—1665) из Тулузы. Задачи, решенные Ферма, и особенно теоремы, высказанные им, но доказательства которых он скрыл по обычаю того времени, произвели большое впечатление на последующих математиков. Ферма имел особую способность проникать в самые глубокие тайны чисел. Укажем два примера. В 1651 г. Ферма, в виде вызова всем современным ему математикам, поставил задачу доказать, что если  $\Delta$  — целое положительное число, отличное от полного квадрата, то уравнение  $x^2 - \Delta y^2 = 1$  (которое теперь называется уравнением Пелля) всегда имеет решения в целых числах  $x, y$  ( $y \neq 0$ ). Теорема эта в руках Эйлера и Лагранжа, который первый ее доказал в 1768 г., оказалась ключом ко всему неопределенному анализу 2-й степени. Другой пример: на полях своего экземпляра книги Диофанта Ферма записал утверждение, что, тогда как сумма двух квадратов целых чисел может быть опять квадратом целого числа, сумма двух кубов или двух одинаковых высших сте-

пений не может быть такой же степенью целого числа (так называемая великая теорема Ферма). Теорема эта в общем виде не доказана и не опровергнута до сих пор, но уже самые попытки ее доказать привели к созданию глубоких теорий.

Большая часть задач, оставленных Ферма последующим поколениям математиков, была решена Эйлером (1707—1783) и Лагранжем (1736—1813), которые также поставили и решили многие дальнейшие собственные задачи. Эйлер, в частности, построил теорию степенных вычетов (см. о них дальше на стр. 897); доказал (в его доказательстве, правда, есть пробел), что уравнение  $x^3 + y^3 = z^3$  не имеет решений в целых числах; нашел на числовых примерах (однако не смог этого доказать), что простые числа  $p$ , такие, для которых заданное целое число  $a$  есть «квадратичный вычет» (т. е. те  $p$ , для которых существуют такие квадраты  $x^2$ , что число  $a$  отличается от них лишь на кратности  $p$ ), суть те и только те простые числа, которые содержатся в некоторых определенных арифметических прогрессиях (так называемый квадратичный закон взаимности в рациональном поле), а также многое и многое другое. Лагранж глубоким и тонким методом доказал утверждение Ферма об уравнении Пелля и показал, что этот метод дает способ для полного решения в целых числах любого неопределенного уравнения 2-й степени с двумя неизвестными  $ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$ . Кроме того, Лагранж доказал замечательную теорему, верность которой утверждал уже Ферма, что любое целое положительное число  $N$  есть сумма четырех квадратов целых чисел:  $N = x^2 + y^2 + z^2 + t^2$ , частный случай так называемой общей теоремы Варинга, доказанной в общем виде только в 1909 г. Гильбертом.

Лежандр (1752—1833) опубликовал первый большой трактат о теории чисел, в котором собрал все сделанное до него и добавил много нового.

Таково было положение теории чисел до Гаусса.

## 2. «Арифметические исследования» Гаусса

Гаусс (1777—1855) с самого раннего возраста обнаруживал необыкновенные способности к математике. Сохранилось предание, что он, когда ему едва минуло 3 года, присутствовал при расчете

своего отца, бывшего водопроводным мастером, с подсобными рабочими и заметил, что расчет сделан неверно, а верно так-то. Расчет был проверен, и присутствующие с неподдельным удивлением увидели, что число, указанное трехлетним мальчиком, правильное. Уже 18 лет Гаусс получил в математике результаты первостепенной важности. С 1797 г. Гаусс начал печатать свою знаменитую книгу «Арифметические исследования» (*«Disquisitiones arithmeticae»*)\*. По тогдашним условиям печатание шло медленно, и в течение этого времени Гаусс дорабатывал разные части книги, особенно пятый ее раздел. «Арифметические исследования» вышли в свет в 1801 г., когда Гауссу было 24 года. «Арифметические исследования» — первая книга, в которой теория чисел, или, как говорит Гаусс, высшая арифметика, излагается как стройная наука, причем во всех вопросах Гаусс обращает особое внимание на принципиальную сторону дела. Книга Гаусса оказывала решающее влияние на работы всех математиков мира по теории чисел в течение целого столетия, а многие идеи, в ней заложенные, оказали влияние на всю математику в целом. Все результаты работ в теории чисел предыдущих ученых, таких, как Ферма, Эйлер, Лагранж, Лежандр, включены в тот или иной из семи разделов, на которые разделено это фундаментальное сочинение, имеющее более 600 страниц, но большей частью эти результаты изложены, исходя из более общих, глубоких и объединяющих принципов. Кроме того, книга содержит в четвертом, пятом и седьмом разделах три совершенно различных первоклассных и фундаментальных для теории чисел и алгебры новых открытия самого Гаусса: 1) доказательство закона взаимности, 2) теорию композиции квадратичных форм и теорию их родов и 3) теорию деления круга. Два других крупнейших открытия Гаусса в теории чисел: 4) гауссовы суммы и 5) арифметика целых комплексных чисел, были сделаны уже позже, после выхода в свет «Арифметических исследований», и опубликованы соответственно в 1811 и в 1828—1832 гг.

Относительно общего стиля «Арифметических исследований» Гаусса надо сказать следующее. Гаусс был несравненным вычисли-

---

\* C. F. G a u s s. Werke, Bd. I; см. также: C. F. G a u s s. Untersuchungen über höhere Arithmetik. Deutsch. hrsg. von H. Maser, 1889.



телем и, подобно тому, как это делали многие другие выдающиеся арифметики, обычно получал свои новые результаты, исходя из обширных численных вычислений, которые позволяли ему подмечать новые, глубоко скрытые арифметические истины, доказательства которых он получал затем нередко лишь в результате упорной, продолжительной, иногда многолетней работы. Книга Гаусса проникнута стремлением решить каждый вопрос так, чтобы получить удобный вычислительный алгоритм. Многие места книги поясняются численными примерами и небольшими численными табличками, которые делают непосредственно ясным то, о чем идет речь и, так сказать, вводят в самую практику рассматриваемых арифметических вопросов.

Когда углубляешься в изучение книги Гаусса, то прямо недоумеваешь, как мог двадцатилетний молодой человек создать такой грандиозный комплекс сложнейших и глубочайших методов и теорем, так хорошо слаженный и построенный и, кроме того, содержащий, как было указано выше, три первоклассных открытия, каждое из которых уже одно обессмертило бы имя любого математика. Несомненно, что умственный подвиг молодого Гаусса, приведший к написанию «Арифметических исследований», имеет мало себе равных в мировой науке.

Попробуем теперь по порядку рассмотреть открытия Гаусса в теории чисел и выяснить то значение, которое каждое из них имело для дальнейшего развития математики. Но прежде, чем это делать, нам придется довольно много сказать о теории чисел вообще и о теории алгебраических чисел в частности.

### 3. О теории чисел вообще и о современных нам ее методах

Обыкновенные целые числа..., — 3, — 2, — 1, 0, 1, 2, 3,... являются основой всей математики. В отношении сложения они образуют весьма простую совокупность (бесконечную циклическую абелеву группу), а именно: ..., — 1—1, — 1, 0, 1, 1+1, 1+1+1, ..., единственным исходным кирпичом которой является число 1. В отношении же к умножению тот же ряд целых чисел имеет уже вовсе не простую

структуру. А именно тех простейших кирпичей, из которых строятся умножением все целые числа, бесконечно много — это простые числа, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... Натуральные числа, большие 1, получаются из них умножением так: 2, 3,  $2 \cdot 2$ , 5,  $2 \cdot 3$ , 7,  $2 \cdot 2 \cdot 2$ ,  $3 \cdot 3$ ,  $2 \cdot 5$ , 11,  $2 \cdot 2 \cdot 3$ , 13,  $2 \cdot 7$ ,  $3 \cdot 5$ ,  $2 \cdot 2 \cdot 2 \cdot 2$ , 17, ... Для того же, чтобы умножением получить все целые рациональные числа, надо еще привлечь обе единицы; 1 и  $-1$  и число 0.

Уже даже самый простой вопрос, как идут в ряду натуральных чисел 1, 2, 3, 4, 5, 6, ... простые числа, до настоящего времени представляет непреодолимые трудности. Со времен Эвклида доказано, что их бесконечно много. Но только Чебышеву в 1849 г. удалось показать, что число  $\pi(N)$  простых чисел, меньших данного предела  $N$ , приблизительно равно  $\frac{N}{\ln N}$ , а затем Адамару и Валле-Пуссену — что отношение  $\pi(N) : \frac{N}{\ln N}$  стремится к пределу 1. Лишь совсем недавно, в 1937 г., И. М. Виноградову в знаменитой работе удалось доказать, что любое достаточно большое натуральное число  $N$  есть сумма четырех простых чисел. Но, например, до сих пор не удается выяснить, встречаются ли сколь угодно далеко так называемые «близнецы», т. е. простые числа, отличающиеся друг от друга на число 2, как пара 101 и 103 или пара 8004119 и 8004121.

Вся трудность теории чисел состоит в том, что свойства целых чисел относительно умножения (мультипликативные свойства) с их свойствами относительно сложения (с их аддитивными свойствами) связаны очень сложно.

Перейдем теперь к рассмотрению современных нам методов теории чисел.

На современном нам этапе теории чисел для решения вопросов теории обыкновенных целых рациональных чисел используются, кроме элементарного, в основном четыре метода:

- 1) теория алгебраических чисел (и других алгебр);
- 2) теория алгебраических функций;
- 3) аналитическая теория чисел;
- 4) геометрия чисел.

Отметим тех главнейших математиков, кроме Гаусса, которые до настоящего времени создавали эти методы.

К использованию метода алгебраических чисел относятся работы Валлиса об уравнении Пелля, работы Лагранжа о неопределенных уравнениях 2-й степени, доказательство Эйлера теоремы Ферма для кубов, работы Эйзенштейна и Куммера о законе взаимности, работы Дирихле о теории единиц, работы Куммера об идеальных числах, работы Дедекинда, Золотарева, Кронекера по теории простых делителей, работы Гильберта, Такаги, Артина, Хассе по теории поля классов, работы Фробениуса и Чеботарева, обобщающие теорему Дирихле о прогрессии, работы Шафаревича об общем законе взаимности и работы Тэта о группах когомологий.

К обобщению этого метода на теорию квадратичных форм с многими переменными относятся работы Венкова, Хассе, Хекке, Зигеля, Витта, Эйхлера.

Основные сводки по этому методу принадлежат Гильберту (1896) — по общей теории алгебраических чисел, Хассе (1924) — по специальному вопросу теории алгебраических чисел, теории поля классов, и Эйхлеру (1952) — по применению алгебр к арифметике квадратичных форм со многими переменными.

Использование теории алгебраических функций, родственной теории алгебраических чисел, но имеющей свои специфические методы, начал Пуанкаре, затем в этом направлении работали Морделл, А. Вейль, Хассе и др.

Аналитическая теория чисел ведет свое начало от Эйлера. Дирихле и Чебышев продолжали развитие этих идей в вещественной области. Новую струю влил Риман, который вышел в комплексную плоскость и начал использовать аналитичность функции и аналитическое продолжение. Методы аналитической теории чисел употребляли в теории алгебраических чисел Дирихле, Дедекинд, Кронекер, Фробениус, Чеботарев, Хекке, Зигель, Хейльбронн и др. Важный прием для аддитивных задач придумал Вороной. Блестящее развитие та же идея, хотя, по-видимому, и независимо от Вороного, получила в работах Рамануджана и Харди и Литтльвуда.

Важной главой аналитической теории чисел является оценка тригонометрических сумм, первый далеко идущий результат в которой был получен в 1914 г. Г. Вейлем. Наиболее глубокие новые идеи в этой области были развиты Виноградовым, который, между

прочим, получил оценки тригонометрических сумм по простым числам.

Основателями геометрии чисел были Минковский, Вороной и Клейн. Ее методами работали у нас автор этих строк и Венков, а также их используют многие современные математики.

Работы Гаусса по теории чисел дают первые образчики почти во всех этих направлениях, но наибольшее значение они имеют для развития метода алгебраических чисел и метода тригонометрических сумм.

#### 4. О теории алгебраических чисел

1. *Основные понятия.* Уже самые первые крупные арифметики, которые пытались решать более глубокие вопросы теории целых чисел, начали убеждаться в том, что часто для их решения надо так или иначе привлекать некоторые вспомогательные, так называемые алгебраические, иррациональности, т. е. корни некоторых уравнений с рациональными коэффициентами. Этот метод играл роль уже в работах Валлиса (1616—1703) об уравнении Пелля, в работах Лагранжа о неопределенных уравнениях 2-й степени, в которых  $\sqrt{\Delta}$  разлагался в непрерывную дробь. В доказательстве невозможности уравнения  $x^3 + y^3 + z^3 = 0$  в целых числах  $x, y, z$  Эйлер привлекает иррациональность  $\sqrt{-3}$  и т. д.

Что же такое поле алгебраических чисел данной степени? Рассмотрим какое-нибудь алгебраическое уравнение  $n$ -й степени с рациональными коэффициентами  $a_1, a_2, \dots, a_n$ :

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n = 0, \quad (1)$$

неприводимое в поле рациональных чисел, т. е. такое, что его левая часть не раскладывается на два множителя низших степеней опять с рациональными коэффициентами, и пусть  $\alpha$  — один из его действительных или комплексных корней. В таком случае число  $\alpha$  называется *алгебраическим числом  $n$ -й степени*. Совокупность  $K$  всех тех чисел, которые получаются из числа  $\alpha$ , если соединять его само с собой любым конечным числом действий сложения, вычитания, умножения и деления, называется *полем алгебраических чисел  $n$ -й степени*, являющимся расширением рационального поля присоеди-

нением к нему числа  $\alpha$ . Можно показать, что присоединение к полю рациональных чисел нескольких алгебраических иррациональностей равносильно присоединению одной такой иррациональности высшей степени.

Легко далее показать, что в силу тождества  $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$  всякое число  $\omega$  поля  $K$ , являющегося результатом присоединения числа  $\alpha$ , можно привести к виду  $\omega = u_1\alpha^{n-1} + u_2\alpha^{n-2} + \dots + u_n$ , где  $u_1, u_2, \dots, u_n$  — рациональные числа, и обратно. Если  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$  все корни уравнения (1), то числа:

$$\begin{aligned} \omega^{(1)} &= u_1\alpha^{(1)n-1} + u_2\alpha^{(1)n-2} + \dots + u_n, \\ \omega^{(2)} &= u_1\alpha^{(2)n-1} + u_2\alpha^{(2)n-2} + \dots + u_n, \\ &\dots\dots\dots \\ \omega^{(n)} &= u_1\alpha^{(n)n-1} + u_2\alpha^{(n)n-2} + \dots + u_n, \end{aligned}$$

которые называются сопряженными между собой, суть все корни некоторого уравнения

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \dots + b_{n-1}x + b_n = 0, \tag{2}$$

также с рациональными коэффициентами  $b_1, b_2, \dots, b_n$ , но которое может уже быть и приводимым (степенью неприводимого).

Нетрудно показать, что все те числа поля  $K$ , для которых в уравнении (2)  $b_1, b_2, \dots, b_n$  — целые рациональные, называемые целыми алгебраическими, образуют в поле  $K$  так называемое кольцо, т. е. такую подсовокупность  $\mathcal{O}$  чисел поля  $K$ , что сумма, разность и произведение ее чисел суть опять ее же числа. Наконец, можно показать, что в этом кольце  $\mathcal{O}$  всех целых чисел поля  $K$  можно выбрать систему  $n$  таких его чисел  $\omega_1, \omega_2, \dots, \omega_n$  — базис кольца  $\mathcal{O}$  всех целых чисел поля  $K$ , — что любое целое число  $\omega$  поля  $K$  имеет вид

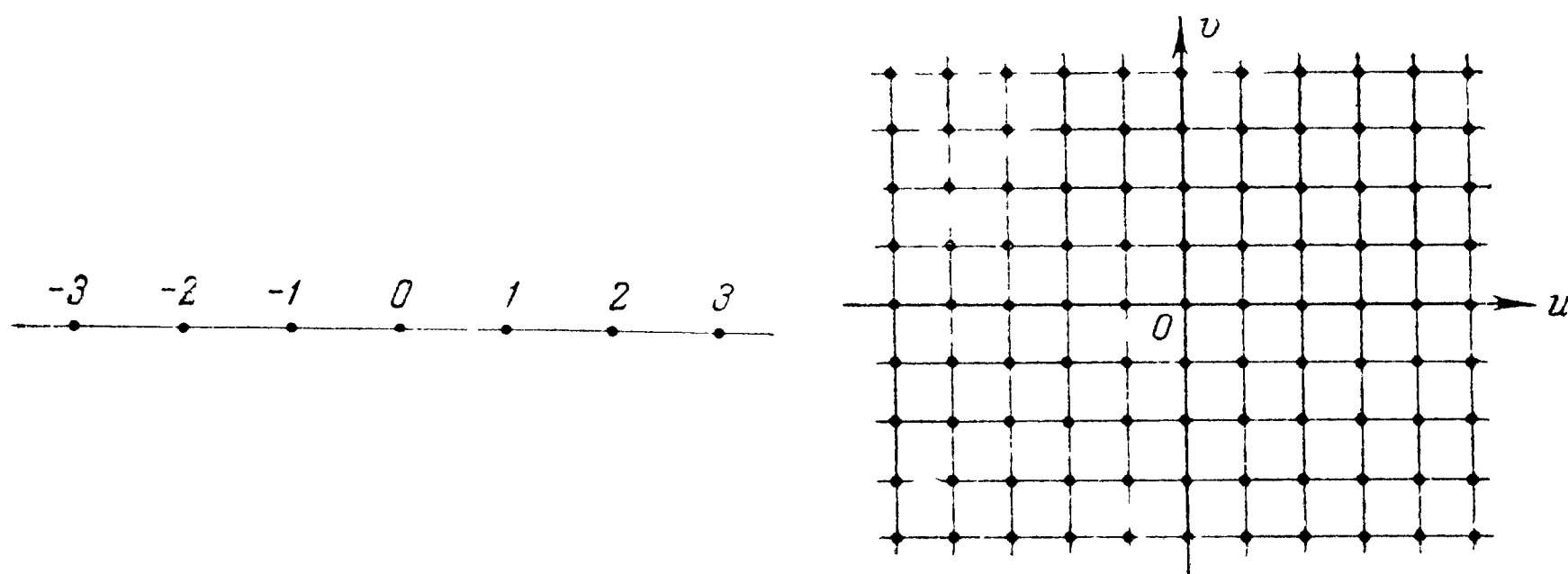
$$\omega = c_1\omega_1 + c_2\omega_2 + \dots + c_n\omega_n,$$

где  $c_1, c_2, \dots, c_n$  — целые рациональные, и обратно.

Арифметика кольца  $\mathcal{O}$  всех целых чисел того или иного поля  $K$  алгебраических чисел и играет часто роль при решении разных вопросов теории целых рациональных чисел.

Все, что сейчас сказано, можно изложить и иначе — геометрически.

2. *Геометрическое изложение.* Начнем с обыкновенных целых рациональных чисел. Возьмем координатную ось и будем называть суммой, разностью и произведением двух точек этой оси точку, координата которой есть сумма, разность или произведение координат этих точек. В таком случае легко видеть, что ряд целых рациональных точек  $\dots, -2, -1, 0, 1, 2, \dots$  представляет собой дискретную,

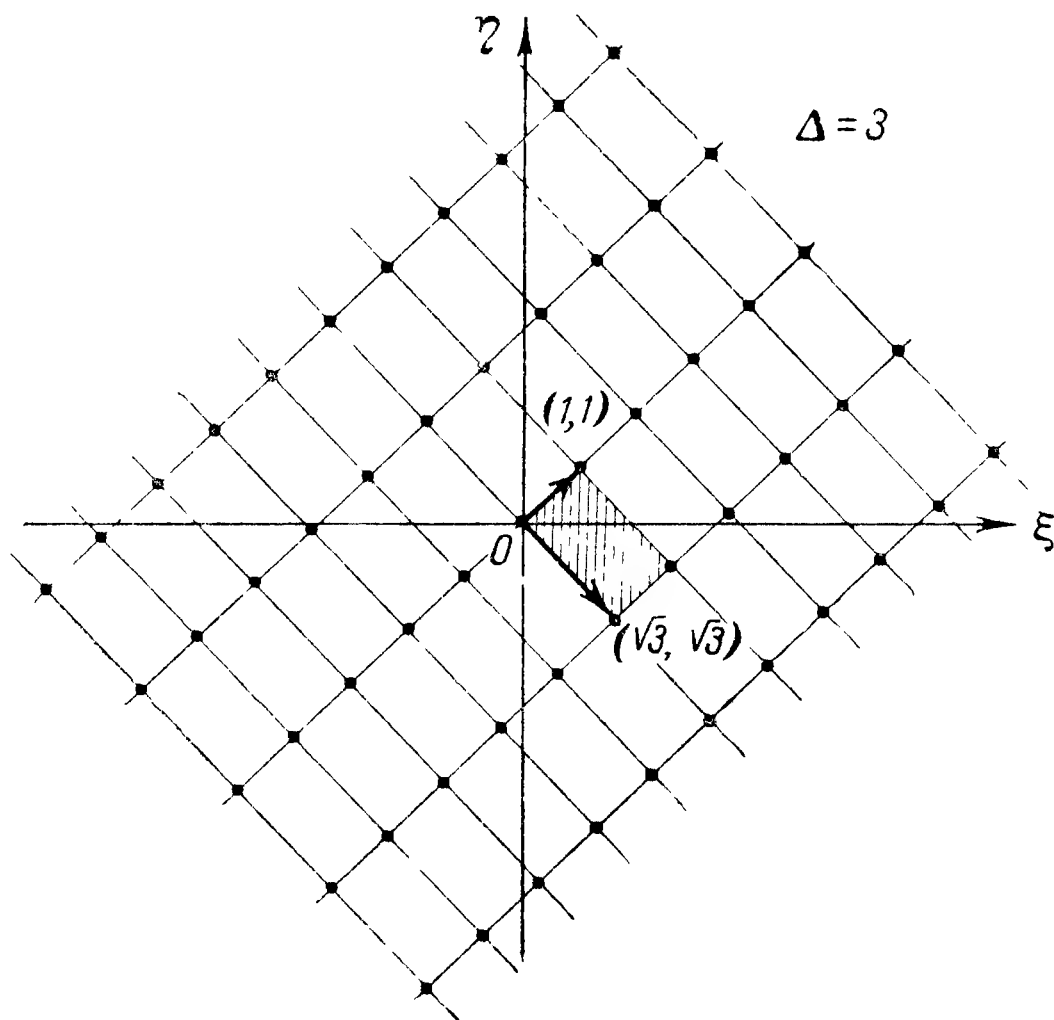


неуплотняемую совокупность точек оси — такую, что такие сумма, разность и произведение ее точек суть ее же точки, и наоборот, если совокупность точек оси обладает этими свойствами (и отличается от одной точки 0), то она есть ряд целых рациональных точек. Неуплотняемость совокупности здесь понимается в том смысле, что нельзя к ней прибавить дальнейших точек так, чтобы старые ее точки вместе с этими новыми опять давали совокупность, удовлетворяющую всем другим потребованным условиям.

Такая совокупность называется *неуплотняемым дискретным кольцом* точек (по отношению к введенным по координатным сложению, вычитанию и умножению).

То же самое можно делать на плоскости, если на ней зафиксирован некоторый заданный координатный репер  $E = Oe_1e_2$  и введено по координатное по отношению к нему сложение, вычитание и умножение точек, так что если, например, заданы точки  $(3, 11)$  и  $(5, -7)$ , то их сумма есть точка  $(8, 4)$ , а произведение — точка  $(15, -77)$ . На плоскости имеется одно очевидное, тривиальное дискретное, неуплотняемое кольцо — это решетка всех точек с целыми рациональными координатами. Действительно, по координатные сумма,

разность и произведение точек этой решетки есть, очевидно, опять точка с целыми рациональными координатами; эта совокупность дискретна и, как нетрудно показать, неуплотняема. Но на плоскости, кроме этого (единственного) приводимого дискретного неуплотняемого кольца, есть еще сколь угодно много других различных колец, которые все уже неприводимы, т. е. не имеют точек на осях координат, кроме начала.

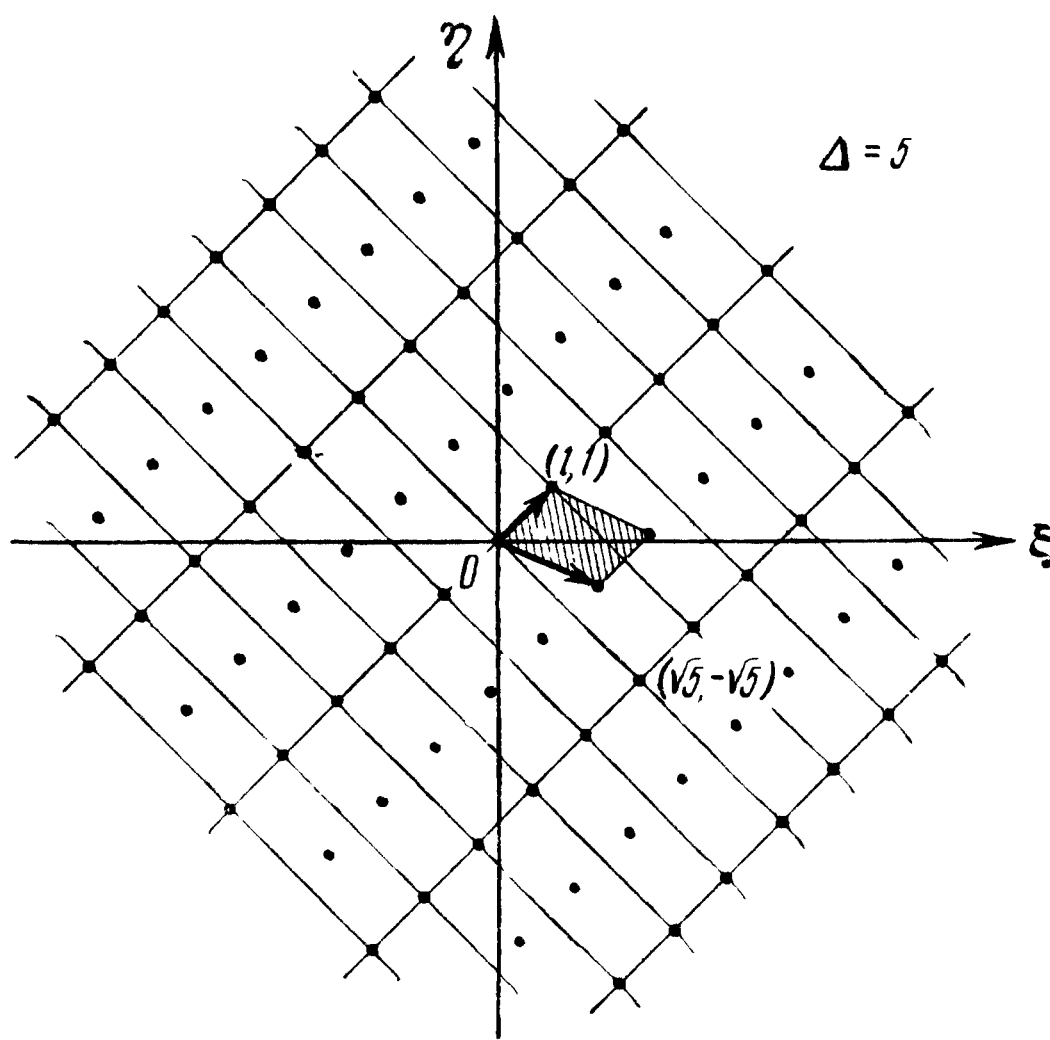


Как можно показать, каждое из них может быть построено так: надо взять любое положительное целое рациональное число  $\Delta$ , не делящееся на квадрат, и рассмотреть репер  $E$ , построенный на векторах  $(1, 1)$  и  $(\sqrt{\Delta}, -\sqrt{\Delta})$ , и решетку точек, на нем построенную (т. е. с целыми рациональными относительно него координатами). Если  $\Delta \not\equiv 1 \pmod{4}$ , то сама эта решетка, представляющая собой решетку прямоугольников, а если  $\Delta \equiv 1 \pmod{4}$ , то та, которая получается из нее, если добавить по точке в центрах всех ее прямоугольников, будет двумерным неприводимым дискретным неуплотняемым кольцом и никаких других таких колец нет.

Можно показать, что каждое из этих колец представляет собой не что иное, как совокупность всех целых чисел некоторого вещественного квадратичного поля алгебраических чисел, если каждому

числу этого поля сопоставлять точку плоскости, координаты которой суть это число и ему сопряженное, и обратно. Квадрат  $d$  площади основного параллелограмма (заштрихованного) такой решетки равен в первом случае  $4\Delta$ , а во втором  $\Delta$ . Он называется *дискриминантом* соответственного квадратичного поля. Итак, дискриминанты вещественных квадратичных полей суть числа  $4 \cdot 2, 4 \cdot 3, 5, 4 \cdot 6, 4 \cdot 7, 4 \cdot 10, 4 \cdot 11, 13, 4 \cdot 14, 4 \cdot 15, 17, 4 \cdot 19, 21, 4 \cdot 22, 4 \cdot 23, 4 \cdot 26, 29, 4 \cdot 30, \dots$ , причем со всяким таким дискриминантом имеется только одно квадратичное поле.

Аналогичное имеет место для  $n$ -мерного вещественного или комплексного пространства, где всякое  $n$ -мерное неприводимое (т. е. не имеющее точек, отличных от точки  $0$ , хоть одна из координат которых равна нулю) неуплотняемое кольцо  $\mathcal{O}$  по отношению к по координатным сложению, вычитанию и умножению есть  $n$ -мерная решетка точек, координатами которых являются целые числа некоторого поля алгебраических чисел  $n$ -й степени и им сопряженные, и обратно. Таких колец  $\mathcal{O}$  бесконечно много, и дискриминанты (квадраты  $n$ -мерных объемов основных параллелепипедов) их суть неубывающие целые числа, причем число различных колец  $\mathcal{O}$  с одним и тем же дискриминантом конечно (теорема Эрмита).





Рассмотрим теперь арифметику такого кольца  $\mathcal{O}$ . В отношении сложения и вычитания такое кольцо построено совсем просто — всякая его точка  $\omega = c_1\omega_1 + c_2\omega_2 + \dots + c_n\omega_n$ , где  $\omega_1, \omega_2, \dots, \omega_n$  суть концы векторов его основного репера  $E$ , а  $c_1, c_2, \dots, c_n$  — целые рациональные числа. Что же касается умножения, то при  $n > 1$  уже вопрос о единицах кольца, т. е. о таких его точках  $\varepsilon$ , от умножения на каждую из которых кольцо  $\mathcal{O}$  переходит само в себя, не так прост. При  $n = 1$  единицы кольца две:  $+1$  и  $-1$ . При  $n > 1$  оказывается единиц, кроме как для квадратичных мнимых полей, бесконечно много, но все они суть произведения степеней конечного числа так называемых основных единиц. Теорема эта была впервые доказана для действительных квадратичных полей Лагранжем в 1768 г., а в общем случае Дирихле в 1846 г., причем в свое время это исследование Дирихле считалось одним из самых трудных в теории чисел.

Далее, в  $\mathcal{O}$  можно выделить так называемые *простые точки*, т. е. такие точки, которые уже нельзя представить в виде произведения нескольких точек  $\mathcal{O}$ , отличных от единиц.

Примеры показывают, что уже при  $n = 2$  существуют кольца  $\mathcal{O}$ , в которых любая точка однозначно разлагается на простые точки (если не учитывать множителей единиц), и существуют другие кольца  $\mathcal{O}$ , в которых это разложение, вообще говоря, неоднозначно. В таких «плохих» кольцах арифметика несовершенна, и они поэтому непосредственно не могут быть успешно использованы. Возможно, что уже и Гаусс знал об этом обстоятельстве. Но не видно было, как от него избавиться, пока Куммер (1810—1893) в 1844 г. для частных случаев полей, зависящих от корней уравнений деления круга  $x^{p-1} + x^{p-2} + \dots + x + 1 = 0$ , где  $p$  — простое число, не показал, что такое кольцо  $\mathcal{O}$  можно дополнить некоторыми так называемыми идеальными элементами так, чтобы в дополненном кольце  $\mathcal{O}^*$  (которое само уже не является кольцом, но является мультипликативной системой, т. е. такой, что произведение любых двух ее элементов есть ее же элемент) разложение было уже однозначно. Позже, в начале 70-х годов, одновременно и независимо друг от друга, разными способами показали то же самое для общего поля алгебраических чисел Дедекин (1831—1916)

и Золотарев (1847—1878). Еще один способ изложить этот вопрос нашел позже Кронекер (1823—1891). Наконец, в 1896 г. Клейн (1849—1925) для частного случая квадратичных полей нашел очень наглядный новый подход, который был впоследствии обобщен на любое поле алгебраических чисел.

3. *Теория идеалов Дедекинда.* Изложим сначала теорию идеалов Дедекинда. Пусть  $L_1$  и  $L_2$  — две  $n$ -мерные подрешетки решетки  $\mathcal{O}$ ; нетрудно доказать, что если составить все попарные произведения их точек и затем рассмотреть все суммы и разности полученных произведений, то получится опять некоторая подрешетка  $L_3$  решетки  $\mathcal{O}$ . Решетка  $L_3$  называется *произведением*  $L_1 L_2$  решеток  $L_1$  и  $L_2$ . Если  $\mathfrak{J}$  такая  $n$ -мерная подрешетка решетки  $\mathcal{O}$ , что  $\mathcal{O}\mathfrak{J} = \mathfrak{J}$ , то  $\mathfrak{J}$  называется *идеалом* в  $\mathcal{O}$ . Очевидно, что если  $\nu$  — точка из  $\mathcal{O}$ , отличная от нуля (т. е. от начала), то решетка  $\mathfrak{J} = \nu\mathcal{O}$ , есть идеал в  $\mathcal{O}$ , так как  $\mathcal{O} \cdot \nu\mathcal{O} = \nu\mathcal{O}$ , ибо  $\mathcal{O}\mathcal{O} = \mathcal{O}$  ввиду того, что в  $\mathcal{O}$  есть точка  $1 = (1, 1, \dots, 1)$  и уже  $1\mathcal{O} = \mathcal{O}$ . Такой идеал  $\nu\mathcal{O}$  называется *главным* идеалом, соответствующим точке  $\nu$ . Дедекиннд показал, что если в  $\mathcal{O}$  нет никаких идеалов, отличных от главных, то любая точка из  $\mathcal{O}$  однозначно, с точностью до множителей единиц, разлагается в произведение простых его точек, т. е. уже в самом кольце  $\mathcal{O}$  арифметика совершенна. Если же в  $\mathcal{O}$  есть идеалы  $\mathfrak{J}$ , отличные от главных, что, как это показывают примеры, бывает очень часто (даже, по-видимому, большей частью, например, для мнимых квадратичных полей всегда, кроме как для конечного числа таких полей), то разложение точек  $\mathcal{O}$  в произведение простых точек  $\mathcal{O}$  уже неоднозначно. Если, однако, вместо точек  $\mathcal{O}$  рассмотреть идеалы в  $\mathcal{O}$ , то оказывается, что среди них имеются простые идеалы, т. е. такие, которые нельзя представить в виде произведения других идеалов, стличных от так называемого единичного идеала  $\mathcal{O}$  ( $\mathcal{O}$ , очевидно, тоже идеал в  $\mathcal{O}$ ), и можно доказать основную теорему, что любой идеал в  $\mathcal{O}$  однозначно разлагается в произведение таких простых идеалов, отличных от единичного идеала  $\mathcal{O}$ .

Два идеала  $\mathfrak{J}_1$  и  $\mathfrak{J}_2$  в  $\mathcal{O}$  называются *эквивалентными*, или *подобными*, если существует такая точка  $\lambda$  в пространстве  $R_n$ , в котором лежит  $\mathcal{O}$ , от умножения на которую один из идеалов переходит в другой, другими словами, если эти идеалы  $\mathfrak{J}_1$  и  $\mathfrak{J}_2$  полу-

чаются друг из друга «растяжениями» по осям координат. Совокупность идеалов  $\mathcal{O}$ , подобных друг другу, образует *класс* идеалов в  $\mathcal{O}$ . Все главные идеалы, очевидно, подобны идеалу  $\mathcal{O}$  — это главный класс. Можно показать, что число  $h$  классов идеалов в  $\mathcal{O}$  конечно.

4. *Теория побочных решеток Клейна.* Перейдем теперь к тому дальнейшему развитию теории Дедекинда, которое предложил Клейн. Оказывается, что если взять по представителю  $\mathfrak{F}_2, \mathfrak{F}_3, \dots, \mathfrak{F}_h$  в каждом из неглавных классов идеалов, то можно их домножить на такие точки  $\lambda_2, \lambda_3, \dots, \lambda_n$  из  $R_n$ , что полученные так называемые побочные решетки  $\mathcal{O}', \mathcal{O}'', \dots, \mathcal{O}^{(h-1)}$  вместе с «главной» решеткой  $\mathcal{O}$  образуют *нормальную фигуру* (Normalfigur)  $\mathcal{O}^*$ , которая уже не есть решетка и обладает следующими свойствами: 1) объемы (вообще говоря, комплексные) основных параллелепипедов всех решеток,  $\mathcal{O}, \mathcal{O}', \mathcal{O}'', \dots, \mathcal{O}^{(h-1)}$  одинаковы; 2) любые две из  $h$  решеток  $\mathcal{O}, \mathcal{O}', \mathcal{O}'', \dots, \mathcal{O}^{(h-1)}$  не имеют общих точек, кроме точки  $\mathcal{O}$ , общей им всем; 3) произведение любых двух точек нормальной фигуры  $\mathcal{O}^*$  есть опять точка этой нормальной фигуры (но сумма двух точек нормальной фигуры, вообще говоря, уже не есть точка нормальной фигуры); 4) произведение любых двух решеток  $\mathcal{O}^{(i)}\mathcal{O}^{(k)}$  есть опять одна из этих решеток  $\mathcal{O}^{(l)}$ , причем таким умножением решетки  $\mathcal{O} \dots \mathcal{O}^{(h-1)}$  образуют абелеву группу, *единицей* которой является  $\mathcal{O}$ ; 5) единицы  $\varepsilon$  главной решетки  $\mathcal{O}$  суть одновременно единицы и каждой из побочных решеток в отдельности и, следовательно, и всей нормальной фигуры  $\mathcal{O}^*$  в целом, причем никаких других единиц нормальная фигура не имеет; 6) всякая точка нормальной фигуры  $\mathcal{O}^*$ , с точностью до множителей единиц, однозначно разлагается в произведение простых точек этой нормальной фигуры.

Связь между теорией идеалов Дедекинда и теорией нормальной фигуры  $\mathcal{O}^*$  Клейна та, что если  $j$  — какая-либо точка нормальной фигуры (отличная от нуля) и  $\mathcal{O}^{(k)}$  — решетка, «обратная» той решетке  $\mathcal{O}^{(l)}$ , в которой эта точка  $j$  лежит, т. е. такая, что  $\mathcal{O}^{(k)}\mathcal{O}^{(l)} = \mathcal{O}$ , то  $j\mathcal{O}^{(k)} = \mathfrak{F}$  есть идеал Дедекинда, лежащий в  $\mathcal{O}$ , соответствующий этой точке  $j$  нормальной фигуры  $\mathcal{O}^*$ , и обратно. Умножению точек  $\mathcal{O}^*$  отвечает умножение соответствующих им идеалов, и обратно

5. *Причины успеха применения алгебраических чисел в теории обыкновенных целых чисел.* Поставим себе вопрос: на каких обстоятельствах основан успех применения алгебраических чисел при решении вопросов об обыкновенных целых числах? Таковых обстоятельств три.

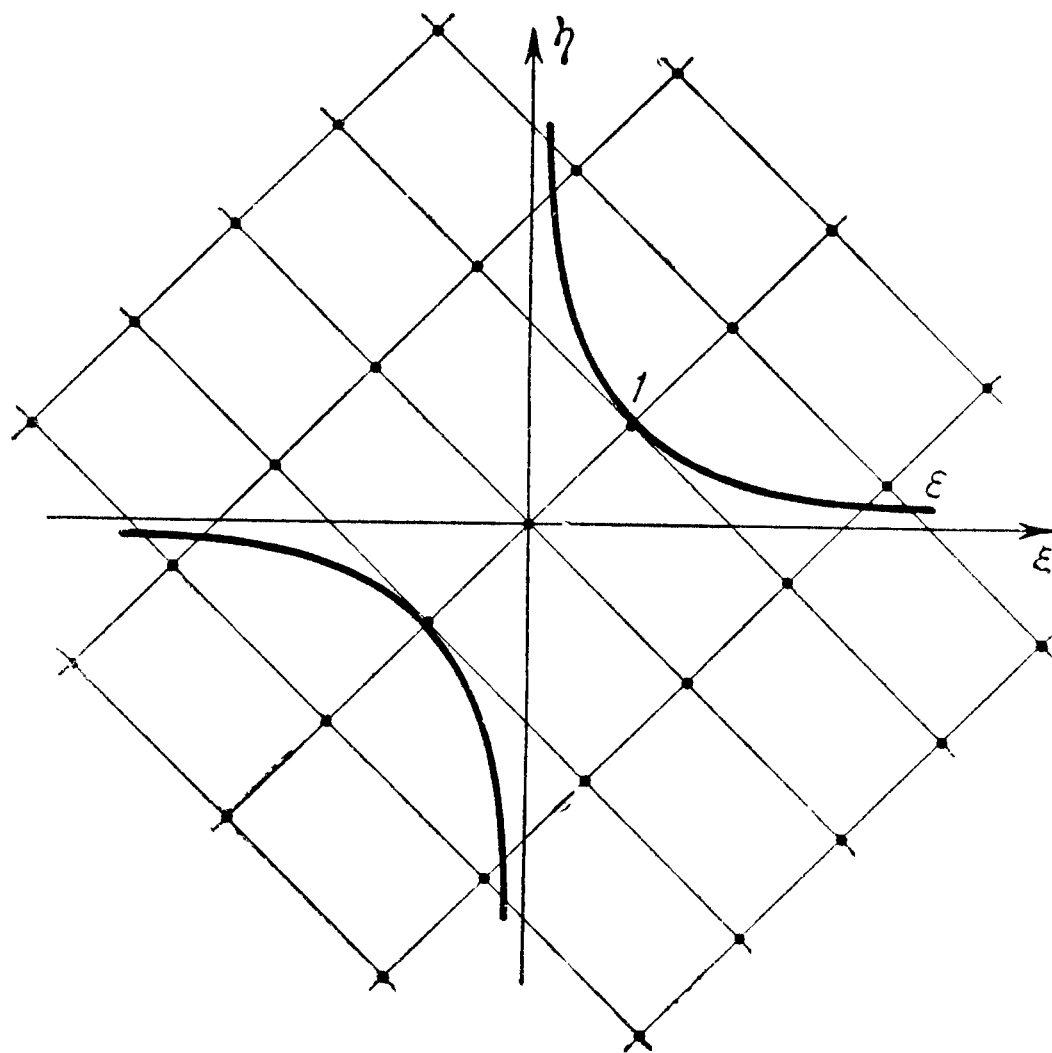
Во-первых, переход в подходящее поле алгебраических чисел часто дает «линеаризацию» задачи. Вместо рассмотрения нелинейного выражения, составленного из обыкновенных целых чисел, рассматриваются его линейные, но иррациональные, алгебраические множители. Пример: уравнение Пелля  $x^2 - \Delta y^2 = 1$  заменяется таким образом  $(x - \sqrt{\Delta}y)(x + \sqrt{\Delta}y) = 1$ , и далее все сводится к рассмотрению линейных выражений  $x - \sqrt{\Delta}y$  и  $x + \sqrt{\Delta}y$ .

Во-вторых, при таком рассмотрении задачи происходит так называемое «распроектирование» задачи, т. е. задачу (которая при непосредственном к ней подходе является, скажем, одномерной) рассматривают в пространстве высшего измерения, где она распутывается. Возьмем тот же пример уравнения Пелля. При переходе к квадратичному полю мы получаем на плоскости решетку точек, соответствующих целым числам этого поля, и вопрос решения уравнения  $x^2 - \Delta y^2 = 1$  сводится к разысканию тех точек в этой решетке, которые лежат на гиперболе  $\xi\eta = 1$ . Отсюда весьма несложно получается знаменитый результат Лагранжа об уравнении Пелля.

В-третьих, заметим следующее. В любом кольце  $\mathcal{O}$  всегда есть точка  $1 = (1, 1, \dots, 1)$ , а следовательно, и точки  $1 + 1 = 2 = (2, 2, \dots, 2)$ ,  $1 + 1 + 1 = 3 = (3, 3, \dots, 3)$  и т. д., так называемые *натуральные точки* кольца  $\mathcal{O}$ . Всякая точка  $\mathcal{O}^*$  есть делитель некоторой натуральной точки  $\mathcal{O}$  (и всех ее кратных, конечно). Всякая простая точка  $\mathcal{O}^*$  есть, оказывается, делитель некоторой натуральной точки  $p$  в  $\mathcal{O}$ , где  $p$  — натуральное простое число, причем такая точка  $p$  разлагается не больше, чем на  $n$  (если  $n$  — степень поля) простых множителей  $\mathcal{O}^*$ . Поэтому для того, чтобы обозреть все простые точки  $\mathcal{O}^*$ , достаточно знать, как разлагается каждое натуральное простое число  $2, 3, 5, 7, 11, 13, 17, \dots$  в произведение простых точек  $\mathcal{O}^*$ .

Мы будем в этом случае говорить, что мы знаем, как *опирается* арифметика того поля алгебраических чисел, кольцом всех

целых чисел которого является  $\mathcal{O}$ , на арифметику поля рациональных чисел. При применении некоторого поля алгебраических чисел к решению какой-нибудь задачи об обыкновенных целых числах обычно очень важно бывает знать закон этого опирания.



Важным обстоятельством является то, что для многих полей алгебраических чисел удастся найти закон этого опирания и что во всех случаях, когда он найден, он весьма простой, конечный; вся же трансцендентная трудность, связанная с простыми точками  $\mathcal{O}^*$ , остается в трансцендентной трудности вопросов распределения обыкновенных натуральных простых чисел  $p$  в ряду всех натуральных чисел.

Например, в квадратичном поле, задаваемом иррациональностью  $\sqrt{\Delta}$ , где  $\Delta$  — некоторое положительное целое рациональное число  $\equiv 1 \pmod{4}$ , не делящееся на квадрат, натуральное простое число  $p$  есть произведение двух простых точек  $\mathcal{O}^*$ , если оно находится в таких-то прогрессиях по модулю  $\Delta$ , и оно есть само простая точка  $\mathcal{O}^*$ , если оно находится в других прогрессиях по модулю  $\Delta$ .

В поле деления круга на  $n$  равных частей, где  $n$  простое, т. е. в поле, зависящем от корня неприводимого уравнения  $x^{n-1} + x^{n-2} + \dots + x + 1 = 0$ , простое натуральное число  $p$  разлагается на простые делители так или иначе в зависимости от того, в какой прогрессии по модулю  $n$  лежит число  $p$ , и т. д.

Мы описали в самых общих чертах и с современной нам точки зрения основные обстоятельства, связанные с теорией алгебраических чисел. Во время Гаусса все это совершенно не было еще известно, и делом Гаусса в теории чисел, в большей его части, было как раз глубоко и последовательно проникать во все эти обстоятельства, исследуя частные, но уже совсем не тривиальные относящиеся сюда вопросы, в основном связанные с теорией квадратичных полей, которые дали важные исходные факты для всех дальнейших исследований в этой области.

Гаусс сам, несомненно, еще не видел всей грандиозной развернутой сейчас картины, но, очевидно, уже предугадывал многие важные ее стороны.

После этого отступления мы можем перейти к подробному последовательному рассмотрению содержания различных разделов «Арифметических исследований» Гаусса.

## 5. Первый, второй и третий разделы «Арифметических исследований» Гаусса

«Арифметические исследования» разделены на 7 разделов (глав), поделенных на мелкие пункты (параграфы), имеющие сквозную нумерацию. Эти пункты мы будем обозначать буквой «п». Всего в «Арифметических исследованиях» 366 пунктов.

Первые три раздела «Арифметических исследований», озаглавленные: 1) «О сравнимости чисел вообще», 2) «О сравнениях первой степени», 3) «О степенных вычетах», представляют собой как бы введение в книгу и не содержат новых открытий, но изложение в них ведется так, что все, до того известное, относящееся к рассматриваемым в них вопросам, приводится в порядок, если нужно, снабжается недостающими доказательствами и т. д.

Уже в первых строках первого раздела «Арифметических исследований» Гаусс вводит новое важное понятие сравнения, которое, по существу, употреблялось, конечно, и до Гаусса, но не было еще никем сформулировано. Это понятие и всем известный удобный значок для него:  $a \equiv b \pmod{m}$ , обозначающий, что числа  $a$  и  $b$  дают одинаковые остатки при делении на модуль  $m$ , вошли с тех пор в теории чисел во всеобщее употребление, так как подчеркивают далеко идущую аналогию между сравнениями и уравнениями.

С более современной точки зрения можно сказать, что введением понятия сравнения положено начало рассмотрению алгебры над конечным полем.

Во втором разделе в п. 16 доказывается однозначность разложения натурального числа на простые множители. По этому поводу Гаусс говорит: «То, что каждое составное число может быть разложено на простые сомножители, известно из основ; однако то, что этого нельзя сделать несколькими различными способами, совершенно необоснованно по большей части предполагается само собой разумеющимся», хотя надо сказать, что эта однозначность уже доказана у Эвклида.

Далее рассматривается решение сравнения 1-й степени

$$ax + t \equiv 0 \pmod{p}$$

и системы таких сравнений.

В п. 42 этого раздела несколько неожиданно вставлено доказательство известной и по настоящее время так часто используемой леммы Гаусса. Если многочлен с целыми рациональными коэффициентами и старшим коэффициентом 1 разлагается в произведение многочленов со старшими коэффициентами, равными 1, и рациональными остальными коэффициентами, то эти коэффициенты тоже целые.

В третьем разделе о степенных вычетах Гаусс, естественно, переходя от сравнений 1-й степени к сравнениям высших степеней, исследует сначала степенные вычеты, т. е. остатки, которые дают степени разных чисел при делении их на данный модуль. Особенно важен случай простого модуля  $p$ . Для каждого числа  $a$ , не делящегося на  $p$ , существует наинизшая степень  $a^d$ , дающая остаток 1.

Число  $d$  — всегда делитель числа  $p - 1$  и называется *показателем*, «к которому принадлежит» число  $a$  по модулю  $p$ .

В пп. 52—57 Гаусс дает способ определить число  $\psi(d)$  не сравнимых по модулю  $p$  чисел, принадлежащих к данному делителю  $d$  числа  $p - 1$ . А именно он показывает, что  $\psi(d) \leq \varphi(d)$ , где  $\varphi$  — число натуральных чисел, меньших  $d$  и взаимно простых с  $d$ . Но если  $d, d', d'', \dots$  — все различные делители  $p - 1$ , то

$$\psi(d) + \psi(d') + \psi(d'') + \dots = p - 1,$$

известно, что

$$\varphi(d) + \varphi(d') + \varphi(d'') + \dots = p - 1,$$

откуда следует, что  $\psi(d) = \varphi(d)$ ,  $\psi(d') = \varphi(d')$  и т. д. и, в частности, что  $\psi(p - 1) = \varphi(p - 1) \neq 0$ .

Таким образом, оказывается доказанным существование первообразных корней  $g$  простого числа  $p$ , т. е. существование таких чисел  $g$ , которые принадлежат к показателю  $p - 1$  по модулю  $p$ . Это доказательство Гаусса является одним из самых блестящих арифметических рассуждений. Существованием первообразного корня  $g$  по простому модулю  $p$  постоянно пользовался Эйлер, однако, по-видимому, он лишь ошибочно считал, что дал доказательство этого существования. Степени  $1, g, g^2, \dots, g^{p-2}$  имеют то свойство, что любое число, не делящееся на  $p$ , сравнимо с одной и только одной из этих степеней по модулю  $p$ .

В 1918 г. И. М. Виноградов показал, что всегда существует первообразный корень простого числа  $p$ , меньший, чем  $2^{2^k} \sqrt{p} \ln p$ , где  $k$  — число различных простых делителей  $p - 1$ .

## 6. Четвертый раздел «Арифметических исследований».

### Первое доказательство закона взаимности

Четвертый раздел «Арифметических исследований» озаглавлен «О сравнениях второй степени». Он содержит знаменитое первое доказательство предложения, называемого в настоящее время *квадратичным законом взаимности* над полем рациональных чисел. Закон этот эмпирически, или, как говорил Гаусс, «индуктивно», впервые был найден Эйлером (см. его статью 1744—1746 гг. «*Theorematum*



*circa divisores numerorum in hac forma  $pa^2 + qb^2$  contentorum*». В форме, почти в точности совпадающей с той, которую придает этой теореме Гаусс, теорема эта была сформулирована Эйлером позже, в 1772 г. (опубликована в «*Opuscula Analytica*» в 1783 г.). Лежандр в «*Histoire de l'Académie Royale des Sciences, Année 1785*» (опубликовано в 1788 г., стр. 465), очевидно, не зная об этих работах Эйлера, снова нашел эту теорему. Однако доказательство этой теоремы не поддавалось всем усилиям Эйлера и Лежандра. Лежандр сам считал, что он ее доказал, но, как справедливо указывает Гаусс, «доказательство» Лежандра содержит предположение о существовании некоторых простых чисел, удовлетворяющих некоторым условиям, доказательства которого Лежандру дать не удалось.

В начале четвертого раздела Гаусс рассматривает вопрос о тех числах  $a$ , которые суть так называемые квадратичные вычеты по заданному модулю  $m$ , т. е. о тех числах  $a$ , для которых сравнение  $x^2 \equiv a \pmod{m}$  имеет решение. Этот вопрос легко сводится к рассмотрению такого же вопроса для того случая, когда модуль — простое число  $p$ , и затем легко решается. В п. 107 раздела 4 Гаусс говорит: «Однако обратная задача: если задано некоторое число, найти все те числа (модули — Б. Д.), по которым оно является (квадратичным — Б. Д.) вычетом или невычетом — значительно сложнее». Эту задачу в силу выше сказанного также достаточно решить для простых модулей  $p$ . Уже Эйлер решил вопрос для  $a = -1$  и 3, а Лагранж — для  $a = 2, 5$  и 7. Знаменитая теорема Эйлера о том, что число  $-1$  есть квадратичный вычет простых чисел  $p$  вида  $4n + 1$  и невычет простых чисел  $p$  вида  $4n + 3$ , была той теоремой, попытка доказательства которой, как об этом свидетельствует сам Гаусс, безвозвратно увлекла его на путь занятия высшей арифметикой. Гаусс решает вопрос о том, для каких модулей данное число  $a$  есть квадратичный вычет, сначала для чисел  $a = -1, \pm 2, \pm 3, \pm 5, \pm 7$ , а затем переходит к доказательству теоремы (закона взаимности), которая решает этот же вопрос для любого числа  $a$ , причем опять достаточно рассмотреть случай, когда заданное число  $a$  простое. Гаусс выражает эту теорему так:

«Если  $p$  — простое число вида  $4n + 1$ , то  $+p$ , а если  $p$  — простое число вида  $4n + 3$ , то  $-p$  будет (квадратичным — Б. Д.) вы-

четом или невычетом каждого простого числа, которое, взятое положительным, является вычетом или невычетом числа  $p$ ».

Гаусс делает вслед за этим следующее замечание: «Так как почти все, что можно высказать о квадратичных вычетах, основывается на этой теореме, то название «фундаментальная теорема», которое мы в дальнейшем будем употреблять, не будет для нее неподходящим».

Доказательство Гаусса основано на полной индукции. Кронекер справедливо называет это доказательство пробой сил Гауссова гения. Наибольшую трудность представил для Гаусса тот пункт этого замечательного доказательства, в котором доказывалось, что для любого простого числа  $a$  вида  $8n + 1$  всегда имеются простые числа, меньшие  $2\sqrt{a} + 1$ , для которых  $a$  — квадратичный невычет. Эта лемма как раз и позволяет Гауссу провести полную индукцию. По словам самого Гаусса, доказательство этой леммы мучило его целый год и противостояло всем его усилиям («per integram annem me tor-sit operamque enixissimam effugit»), пока наконец, ему не удалось решить вопроса при помощи совершенно элементарного, но глубокого соображения, изложенного в п. 129 менее чем на одной странице. Лишь более 100 лет после появления «Арифметических исследований» Гаусса И. М. Виноградову удалось выяснить природу таких лемм и дать целый комплекс теорем, к ним относящихся.

Фундаментальная теорема дает, как это показывает Гаусс в п. 147, полное решение поставленной задачи: найти те простые числа  $p$ , для которых заданное число  $A$  есть квадратичный вычет.

Действительно, пусть, например,  $A$  — некоторое заданное целое положительное число  $\equiv 1 \pmod{4}$ . Разложим  $A$  на простые множители и припишем тем из них, которые вида  $4n + 1$ , знак  $+$ , а тем, которые вида  $4n - 1$ , знак  $-$ , и пусть они, взятые с такими знаками, суть  $a, b, c, d, \dots$ ; тогда произведение  $abcd \dots$  равно  $A$ . Обозначим через  $r, r', r'', \dots$  те целые числа, которые меньше  $A$  и взаимно простые с  $A$  и каждое из которых — квадратичный невычет четного числа чисел  $a, b, c, d, \dots$ . Тогда, как это легко вывести из фундаментальной теоремы, прогрессии  $Ak + r, Ak + r', Ak + r'', \dots$  содержат все те и только те простые числа  $p$ , по которым число  $A$  есть квадратичный вычет.

Для случаев других видов  $A$  результаты совершенно аналогичны.

В последнем п. 152 четвертого раздела Гаусс, используя закон взаимности, дает полное решение общего сравнения второй степени:

$$ax^2 + bx + c \equiv 0 \pmod{m}.$$

Отметим, что Лежандр еще до Гаусса ввел символ  $\left(\frac{a}{p}\right)$  (*символ Лежандра*), определив его так:  $\left(\frac{a}{p}\right) = +1$ , если  $a$  — квадратичный вычет  $p$ , и  $\left(\frac{a}{p}\right) = -1$ , если  $a$  — квадратичный невычет. При помощи этого символа фундаментальная теорема записывается так:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

где  $p$  и  $q$  — два нечетных простых числа. Формула эта обычно называется *законом взаимности двух простых чисел*.

## 7. Целые комплексные числа Гаусса и биквадратичный закон взаимности

В пятом разделе Гаусс дал второе доказательство квадратичного закона взаимности, а впоследствии — еще 6 других его доказательств, основанных на различающихся между собой соображениях. Затем Гаусс в течение многих лет работал над отысканием кубического и биквадратичного законов взаимности, т. е. над решением вопроса о том, каковы те простые числа  $p$ , для которых заданное число  $A$  есть вычет 3-й или 4-й степени, т. е. сравнение  $x^3 \equiv A \pmod{p}$  или  $x^4 \equiv A \pmod{p}$  имеет решение. О кубическом законе взаимности Гаусс ничего не опубликовал и только в 1828 г. напечатал первую свою работу о биквадратичных вычетах, содержащую частные результаты, а в 1832 г. — свою знаменитую вторую работу о биквадратичных вычетах. В этой работе он говорит, что хотя «индукция приносит нам богатый урожай специальных теорем (о биквадратичных вычетах — *Б. Д.*)...; однако между ними отсутствует общая связь...». В п. 1 первой статьи Гаусс говорит: «Намного труднее (чем теория квадратичных вычетов — *Б. Д.*), однако, теория кубических и

биквадратичных вычетов. После того как мы начали исследовать эти вопросы в 1805 г., . . . мы скоро пришли к убеждению, что применявшиеся до сих пор арифметические принципы ни в каком случае не достаточны для обоснования общей теории, а что эта теория с необходимостью требует в некотором смысле бесконечно расширить область высшей арифметики; а как это следует понимать, будет показано в процессе настоящих исследований». Это же утверждение Гаусс повторяет в п. 30 второй статьи, начиная с которого он и приступает к этому «расширению поля арифметики».

Гаусс вводит кольцо  $\mathcal{O}$  так называемых *целых комплексных чисел*  $a + bi$ , где  $a$  и  $b$  — все возможные целые рациональные числа. Другими словами, Гаусс предлагает рассматривать целые числа квадратичного поля, происходящего от присоединения к полю рациональных чисел числа  $i = \sqrt[4]{-1}$ , т. е. корня неприводимого квадратного уравнения  $x^2 + 1 = 0$ . Произведение такого числа на ему сопряженное  $(a + bi)(a - bi) = a^2 + b^2$  называется *нормой* числа  $a + bi$ . Гаусс показывает, что единицами кольца  $\mathcal{O}$  являются числа  $1, i, -1, -i$  (и только они). Далее он показывает, что простыми числами этого кольца являются: 1) числа  $a + bi$ , нормы которых — рациональные простые числа вида  $4n + 1$ , и 2) сами рациональные простые числа  $p$  вида  $4n + 3$ . Наконец, Гаусс доказывает, что любое число  $a + bi$  рассматриваемого кольца  $\mathcal{O}$ , с точностью до множителей  $1, i, -1, -i$ , однозначно раскладывается в произведение таких простых чисел. Таким образом, в смысле вышеизложенной теории алгебраических чисел оказывается, что в этом кольце число классов  $h = 1$ .

После всего этого Гауссу уже удастся, опираясь на численные примеры, сформулировать основную теорему о вычетах 4-й степени (т. е. биквадратичный закон взаимности) для чисел рассматриваемого кольца  $\mathcal{O}$ , причем опять достаточно это сделать только для простых чисел этого кольца. Сам Гаусс в своем мемуаре, однако, доказательства этой теоремы не дает, и не известно, обладал ли он этим доказательством. Доказательство этой теоремы непосредственно в духе идей Гаусса было дано Бушем в начале XX в. Вообще же биквадратичный и кубический законы взаимности были доказаны в первой половине XIX в. Эйзенштейном (из теории комплексного умножения

специальных эллиптических функций) и Якоби (из соображений, связанных с теорией деления круга).

Важность этого второго мемуара Гаусса о биквадратичных вычетах заключается, конечно, не в нахождении биквадратичного закона взаимности, а в том «расширении поля арифметики», о котором говорит Гаусс. Вся трудность была в том, чтобы понять, что простой вид теория биквадратичных вычетов приобретает только в поле  $\sqrt[4]{1}$ , и показать, что в этом поле такая же простая арифметика, как в поле рациональных чисел. Этим был сделан существенный шаг в построении метода алгебраических чисел, хотя обе главные его трудности — общая теорема о единицах и теория идеальных делителей — в этом простейшем случае не были еще затронуты.

## 8. О законах взаимности вообще и о задаче, которую они решают

Что представляют собой законы взаимности с точки зрения той схемы применения метода алгебраических чисел, которую мы рассмотрели в параграфе 4? Начнем с самого простого: квадратичного закона взаимности над полем рациональных чисел.

Можно показать, что в квадратичном поле с дискриминантом  $d$ , т. е. в поле, получаемом от присоединения к полю рациональных чисел корня  $\alpha$  неприводимого квадратного уравнения  $x^2 + ax + b = 0$  с рациональными коэффициентами  $a$  и  $b$ , если  $\Delta$  — целое рациональное число, не делящееся на квадрат, и такое, что оно отличается от числа  $\frac{a^2}{4} - b$  целым или дробным квадратным множителем и  $d = \Delta$ , если  $\Delta \equiv 1 \pmod{4}$ , и  $d = 4\Delta$ , если  $\Delta \equiv 2$  или  $3 \pmod{4}$ , простое число  $p$  следующим образом раскладывается на простые делители:

1)  $p$  разлагается на два разных простых идеальных делителя, если  $\left(\frac{d}{p}\right) = +1$ ;

2)  $p$  — само простой идеальный делитель, если  $\left(\frac{d}{p}\right) = -1$ ;

3)  $p$  есть квадрат простого идеального делителя, если  $p$  — множитель  $d$ , причем можно легко найти и сами соответственные простые идеальные делители.

Таким образом, содержится или не содержится простое число  $p$  в тех прогрессиях, которые были из квадратичного закона взаимности выведены на стр. 899, решает вопрос об «опирании» арифметики квадратичного поля на арифметику поля рациональных чисел. Наоборот, можно показать, что, зная законы разложения натуральных простых чисел в квадратичных полях, можно из них вывести закон взаимности.

Только в свете этого обстоятельства, показывающего, что квадратичный закон взаимности есть то главное звено, которое делает возможным полноценное употребление квадратичного поля для решения соответственных вопросов теории обыкновенных целых чисел, ясно, почему Гаусс придавал ему такое большое значение, и предложил до восьми различных его доказательств.

После Гаусса многие математики упорно занимались отысканием законов взаимности для вычетов высших степеней. Мы уже указывали, что кубический и биквадратичный законы взаимности доказали Якоби и Эйзенштейн. Закон взаимности для вычетов  $p$ -х степеней между рациональным простым числом  $q$  и простым делителем поля  $R(\sqrt[p]{1})$  нашел тоже Эйзенштейн. Много лет работы посвятил разысканию доказательства общего закона взаимности для вычетов  $p$ -х степеней в поле  $R(\sqrt[p]{1})$  создатель теории идеальных делителей Куммер, причем в этих исследованиях Куммер наткнулся на важность некоторой логарифмической производной, появление которой в теории чисел казалось совершенно необъяснимым. Долгое время закон взаимности Куммера считался крайним, чего удастся достигнуть на этом пути. Но многие математики и дальше упорно занимались разысканием еще более общих законов взаимности. Наибольший успех был достигнут в этом вопросе знаменитым немецким математиком Гильбертом (1862—1943) и его школой. Гильберт показал при помощи теории поля классов (о которой будет речь в следующем параграфе), что правая часть равенства, записывающего закон взаимности, может быть представлена как произведение конечного числа некоторых символов, которые он назвал «норменными символами» и простейшие свойства которых он установил. Однако дать прямую конструкцию этих символов, т. е. их явное функциональное

выражение через числа, стоящие в левой части равенства, и характеристики поля ему не удалось. Это было сделано в самые последние годы советским математиком И. Р. Шафаревичем, который, основываясь на новых идеях, дал, наконец, полное решение вопроса, а именно нашел и доказал общий закон взаимности. Между прочим, в методе Шафаревича логарифмическая производная Куммера получила естественное объяснение. Таким образом, знаменитый вопрос, у начала которого стоят гениальные работы Гаусса, наконец, решен окончательно.

Каков же смысл, в свете схемы § 4, всех этих законов взаимности? Все они суть частные случаи закона взаимности Шафаревича, следовательно, достаточно разобрать, каков его смысл. Закон взаимности Шафаревича решает следующий вопрос: если задано любое поле  $k$  алгебраических чисел  $m$ -й степени, содержащее корень  $n$ -й степени из 1, и оно расширяется до поля  $K$  присоединением к нему  $\sqrt[n]{\omega}$ , где  $\omega$  — число поля  $k$ , узнать, как опирается арифметика поля  $K$  на арифметику поля  $k$ . Квадратичный закон взаимности, как мы сейчас видели, решает этот вопрос для того частного случая, когда  $k$  — поле рациональных чисел и  $n = 2$ ; кубический и биквадратичный законы взаимности Эйзенштейна и Якоби — для частного случая, когда  $k$  — поле деления круга на 3 или 4 равные части и  $n = 3$  или 4; закон взаимности Куммера — для частного случая, когда  $n = p$  и  $k$  — поле деления круга на  $p$  частей.

## 9. О теореме Кронекера и о теории поля классов

Легко показать, что всякое квадратичное поле есть подполе некоторого поля деления круга. Еще в 1854 г. Кронекер наметил доказательство одной из самых замечательных теорем всей алгебры — корень любого уравнения с рациональными коэффициентами, группа Галуа которого абелева (коммутативная), выражается рационально через некоторый корень из 1. Это, несомненно, самая красивая теорема теории Галуа, доказанная после Галуа. Таким образом, весьма просто описываются все абелевы (т. е. с абелевыми группами Галуа) расширения рационального поля — все они суть подполя полей деления круга, и обратно. Ввиду того, что вопрос о том, как опи-



рается арифметика поля деления круга на арифметику рационального поля, решается совсем просто, а тогда уже просто решить этот вопрос для любого подполя поля деления круга, теорема Кронекера решает вопрос об опирании на арифметику рационального поля для любых абелевых расширений поля рациональных чисел. Рациональные простые числа  $p$  так или иначе разлагаются в произведение простых делителей данного абелева поля в зависимости от того, заключаются ли они или не заключаются в таких-то прогрессиях. Теорема о разложении натуральных простых чисел  $p$  в квадратичном поле, указанная выше, есть просто частный случай этой общей теоремы, так как квадратичное поле абелево.

Так как всякое абелево расширение поля рациональных чисел  $p$ -й степени над полем корня  $p$ -й степени из 1 получается присоединением одного  $\sqrt[p]{\omega}$ , где  $\omega$  — число этого поля, а арифметика таких расширений регулируется законом взаимности Куммера, обратно из этого закона взаимности можно получить теорию абелевых расширений рационального поля, включая теорему Кронекера, как это было сделано в 1915 г. автором этих строк. Понадобился даже, только более простой, закон взаимности Эйзенштейна, а для циклических полей степени  $p^k$  — закон взаимности Вестерна.

Полное доказательство теоремы Кронекера дал только Вебер в 1886 г.\* Позже, начиная с 1892 г., сначала на наиболее простом случае относительно квадратичных полей, Гильберт начал развивать общую теорию поля классов, т. е. теорию классификации и теорию опирания арифметик относительно абелевых расширений  $K$  любого заданного поля  $k$  (а не только рационального) алгебраических чисел. После углубленных работ самого Гильберта, Фуртвенглера и японского математика Такаги такая теория была построена. Важную теорему, опираясь на один метод, употребленный для другой цели Н. Г. Чеботаревым, дал в этой теории Артин. Более отработанное изложение дал Хассе, а затем, из иных принципов, — французский математик Шевалле.

Теорема Кронекера и связанная с ней теория есть частный случай общей теории поля классов, а именно: это теория полей классов

---

\* Acta Math., 8.



для того случая, когда  $k$  — поле рациональных чисел. Подобно тому, как эта частная теория поля классов может быть получена из закона взаимности Эйзенштейна или Вестерна (как это было указано выше), общая теория поля классов может быть получена из общего закона взаимности Шафаревича. Это было показано учеником И. Р. Шафаревича — А. И. Лапиным.

## 10. Первая часть пятого раздела «Арифметических исследований»

Пятый раздел «Арифметических исследований» Гаусса (пп. 153—307), озаглавленный «О формах и неопределенных уравнениях второй степени», посвящен теории квадратичных форм. Этот раздел самый обширный из семи разделов и необыкновенно богат содержанием. Он, естественно, разделяется на 4 части. Первая его часть (пп. 153—222) содержит классификацию и теорию представления чисел двойничными квадратичными формами, а также решение в целых числах общего неопределенного уравнения 2-й степени с двумя неизвестными. Вторая его часть (пп. 223—265), озаглавленная «Дальнейшие исследования о формах», содержит теорию композиции классов двойничных квадратичных форм и теорию их родов. Третья часть (пп. 266—285), озаглавленная «Отступление, содержащее исследование о тройничных формах», посвящена теории тройничных квадратичных форм. Четвертая часть (пп. 286—307), озаглавленная «Некоторые приложения к теории двойничных форм», содержит доказательство теоремы о родах, теорию разложения чисел в сумму трех квадратов или трех треугольных чисел, решение неопределенного уравнения  $ax^2 + by^2 + cz^2 = 0$ , решение общего неопределенного уравнения 2-й степени с двумя неизвестными в рациональных числах и соображения о среднем числе классов в роде.

Все, что изложено в первой части пятого раздела, в принципе было уже сделано до Гаусса, в основном Лагранжем, однако изложение Гаусса формально (но не по существу) сильно отличается от изложения Лагранжа.

1. Сведение основных задач теории целочисленных двойничных квадратичных форм к задаче об эквивалентности двух таких форм.

Выражение вида

$$ax^2 + 2bxy + cy^2,$$

т. е. двойничную квадратичную форму, Гаусс называет формой 2-степени, или просто *формой*, и обозначает  $(a, b, c)$ . Коэффициенты  $a, b, c$  предполагаются целыми рациональными. Если существуют такие целые рациональные  $x = m, y = n$ , что  $am^2 + 2bmn + cn^2 = M$ , то число  $M$  называется *представимым формой*  $(a, b, c)$ . Число  $D = b^2 - ac = -\begin{vmatrix} a & b \\ b & c \end{vmatrix}$  называется *определителем* формы. Пусть  $m, n$  — примитивное представление числа  $M$ , т. е.  $m$  и  $n$  взаимно простые, и пусть  $\mu$  и  $\nu$  — такие целые рациональные числа, что  $\mu m + \nu n = 1$ ; тогда  $b^2 - ac \equiv [\mu(mb + nc) - \nu(ma + nb)]^2 \pmod{M}$ , что следует из тождества

$$\begin{aligned} (am^2 + 2bmn + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2) &= \\ &= [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac)(m\mu + n\nu)^2. \end{aligned}$$

Определитель  $D = b^2 - ac$  формы есть, следовательно, квадратичный вычет каждого представляемого ею числа  $M$ . Каждое примитивное представление числа  $M$ , как легко показать, независимо от выбора чисел  $\mu$  и  $\nu$ , «принадлежит» к некоторому определенному «значению»  $\nu$  выражения

$$\sqrt{b^2 - ac} \pmod{M}.$$

После этих вводных замечаний излагается теория линейных и линейных унимодулярных преобразований двойничной квадратичной формы  $F$

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

в форму  $F'$ .

Выводится формула

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2,$$

т. е. то правило, что определитель преобразованной формы равен определителю преобразуемой формы, помноженному на квадрат определителя преобразования.

Формы  $F$  и  $F'$  называются *собственно эквивалентными* (*proprie aequivalentes*), если  $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = +1$ , и *несобственно эквивалентными* (*improprie aequivalentes*), если  $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = -1$ .

Лагранж не различал собственной от несобственной эквивалентности. Он считал две формы эквивалентными, если одна переходит в другую при помощи линейной подстановки с определителем  $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$ , равным  $+1$  или  $-1$ , все равно.

Таким образом, класс эквивалентных форм Лагранжа составляет два класса Гаусса, т. е. классификация Гаусса более дробная. Если рассматривать то геометрическое толкование, которое мы разбираем ниже, то собственно эквивалентным формам соответствуют одинаково ориентированные основные реперы решетки, соответствующей классу форм, а несобственно эквивалентным — равно ориентированные, т. е. при помощи различения этих понятий можно учитывать относительную ориентацию реперов. Но различение Гауссом собственной и несобственной эквивалентностей имело, по-видимому, в основном другую, более глубокую причину. Дело в том, что композиция квадратичных форм, которую Гаусс вводит во второй части пятого раздела и которая имела такое капитальное значение для развития как теории чисел, так и алгебры, как это будет нами показано, даст стройную теорию, только если рассматривать эквивалентность в этом более узком смысле, по Гауссу, так как только в этом случае можно говорить не о композиции форм, а о композиции классов.

После введения всех указанных выше понятий Гаусс ставит две основные задачи:

1. Если даны две формы  $F$  и  $F'$  с одним и тем же определителем  $D$ , узнать, эквивалентны ли они и притом собственно или несобственно, а если с разными определителями, то не содержит ли одна форма другую, и найти все собственные и несобственные преобразования одной формы в другую.

II. Если дана форма  $F$ , узнать, представляется ли ею число  $M$ , и найти все такие представления, если они есть.

При этом Гаусс доказывает теорему: если число  $M$  представляется формой  $ax^2 + 2bxy + cy^2$  при  $x = t$ ,  $y = n$ , где  $t$  и  $n$  взаимно

простые, и если «значение» выражения  $\sqrt{D} \pmod{M}$ , к которому принадлежит это представление, равно  $N$ , то формы  $F = (a, b, c)$  и  $G = (M, N, \frac{N^2 - D}{M})$  — собственно эквивалентны, и  $F$  переходит в  $G$  при помощи подстановки:

$$x = tx' + \nu y', \quad y = nx' + \mu y', \quad (1)$$

где  $\mu$  и  $\nu$  находятся из уравнений:

$$t\mu + n\nu = 1, \quad \mu(bt + cn) - \nu(at + bn) = N.$$

Наоборот, если  $F$  и  $G$  эквивалентны и  $G$  получается из  $F$  подстановкой (1), то  $x = t$ ,  $y = n$  есть представление числа  $M$  формой  $F$ , принадлежащее «значению»  $\sqrt{D} \pmod{M}$ , равному  $N$ .

Таким образом, решение задачи II сводится к решению задачи I.

2. *Теория приведения Гаусса для случая определенной двойничной квадратичной формы.* Рассмотрим более подробно решение первого основного вопроса, к которому в конечном счете сводятся все задачи, решаемые в первой части пятого раздела. Подобно тому, как это делал уже и Лагранж, этот первый вопрос Гаусс решает при помощи алгоритма последовательного преобразования заданных форм к эквивалентным им, так называемым приведенным формам. Вопрос этот, естественно, решается совсем разное для случаев, когда  $D < 0$  и когда  $D > 0$ .

Однако Гаусс формально в обоих случаях прибегает к одному и тому же средству: к вычислению последовательных соседних справа форм, — что очень красиво. *Формой соседней справа* (contigua a parte prima) к форме  $(a, b, a')$  Гаусс называет форму  $(a', b', a'')$ , которая получается из формы  $(a, b, a')$  подстановкой  $\begin{vmatrix} 0 & 1 \\ -1 & \delta \end{vmatrix}$ , где  $\delta$  — некоторое целое число.

Для случая  $D < 0$ ,  $a > 0$ , т. е. когда форма положительная определенная, Гаусс показывает, что если выбирать  $\delta$  каждый раз так, чтобы  $b' = -b + a'\delta$  заключалось между  $-\frac{a'}{2}$  и  $\frac{a'}{2}$ , т. е. чтобы было  $2|b'| \leq a'$ , и строить такую форму  $(a', b', a'')$ , соседнюю с заданной  $(a, b, a')$  справа, а затем, далее, такую же форму  $(a'', b'', a''')$ , соседнюю с  $(a', b', a'')$  справа, и т. д., то после конечного числа шагов получится форма  $(A, B, C)$ , эквивалентная данной, для которой

выполняются так называемые неравенства приведения:

$$2|B| \leq A \leq C. \quad (1)$$

Такая форма  $(A, B, C)$  называется *приведенной*. Гаусс далее показывает, что, кроме двух специальных случаев, две формы эквивалентны тогда и только тогда, когда эквивалентные им приведенные формы тождественны.

Все это становится гораздо более прозрачным, если это рассматривать геометрически. Возможно, что уже при писании «Арифметических исследований» и сам Гаусс рассматривал многое в теории квадратичных форм геометрически, как это думает, например, Бахманн, хотя геометрию квадратичных форм, которую мы сейчас рассмотрим, Гаусс и обнародовал гораздо позже, лишь в 1831 г.

Всякая положительная (т. е. если  $D = b^2 - aa' < 0$ ,  $a > 0$ ) двойничная квадратичная форма  $(a, b, a')$  с действительными коэффициентами есть (если говорить современным языком), как легко показать, скалярный квадрат линейного векторного выражения, т. е.

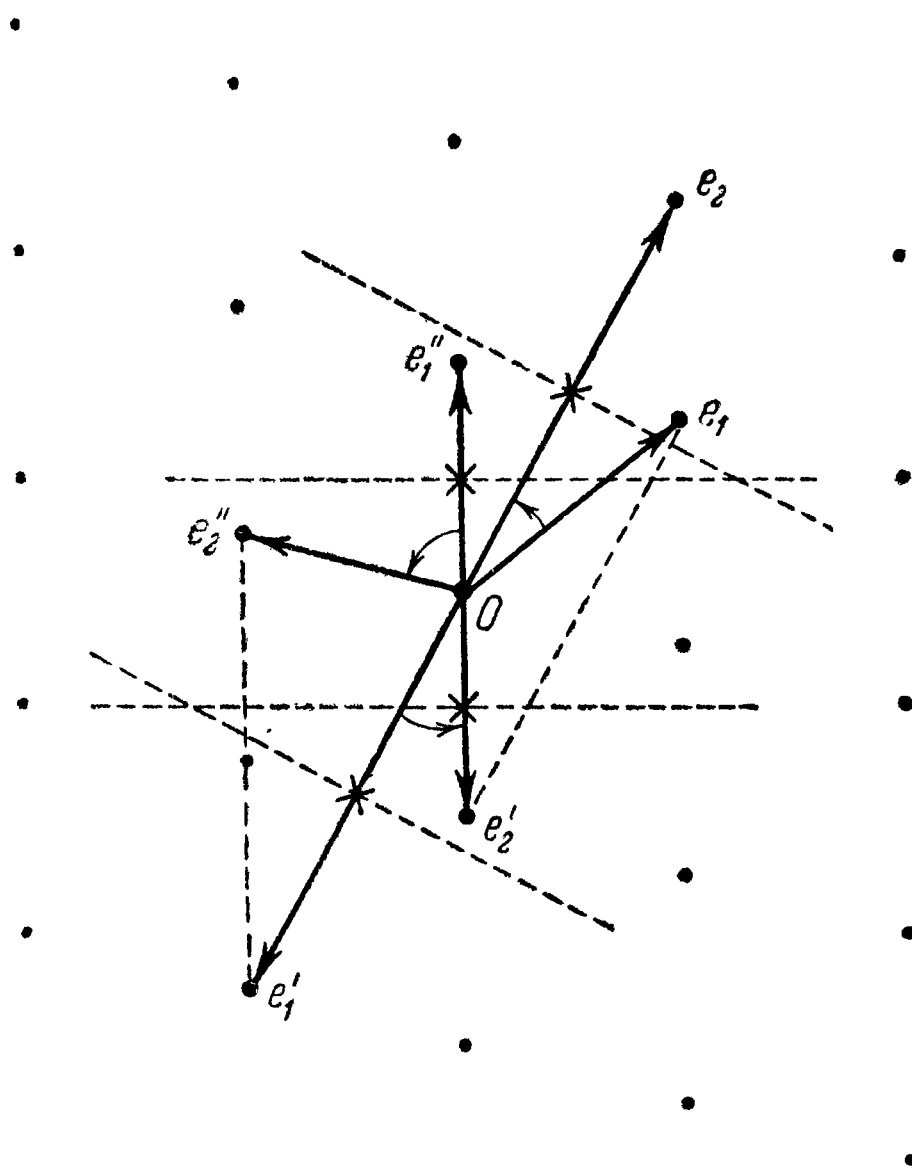
$$\begin{aligned} ax^2 + 2bxy + a'y^2 &= (e_1x + e_2y)^2 = \\ &= |e_1|^2x^2 + 2|e_1||e_2|\cos\varphi xy + |e_2|^2y^2, \end{aligned}$$

где  $|e_1|$ ,  $|e_2|$  — длины векторов  $e_1$  и  $e_2$ , а  $\varphi$  — угол между ними. Построим решетку  $\Gamma$  на репере  $Oe_1e_2$ , т. е. совокупность всех точек плоскости, координаты которых относительно репера  $Oe_1e_2$  целые рациональные.

Переход к форме  $(a', b', c')$ , эквивалентной форме  $(a, b, c)$ , состоит в переходе от репера  $Oe_1e_2$  к другому основному реперу  $Oe'_1e'_2$  той же решетки  $\Gamma$ , а именно, если  $(a', b', c') = (a, b, c) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ , то  $e'_1 = \alpha e_1 + \gamma e_2$  и  $e'_2 = \beta e_1 + \delta e_2$ , и обратно, причем, если форма собственно (proprie) эквивалентна, т. е.  $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = +1$ , то этот новый репер  $Oe'_1e'_2$  имеет ту же ориентацию, как заданный  $Oe_1e_2$ , если же неособенно (improprie) эквивалентна, т. е.  $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = -1$ , то — обратную. Таким образом, классу собственно эквивалентных форм соответствует совокупность всех основных реперов рассматриваемой решетки  $\Gamma$  одной и той же ориентации. Как говорят, решетке соот-

ветствует класс форм, и обратно. То же самое имеет место и в далее рассматриваемой геометризации неопределенных форм, а также в том и другом случае, если коэффициенты  $a, b, c$  не считать целыми, а любыми действительными числами. Форме  $(a', b', a'')$ , соседней справа с формой  $(a, b, a')$ , т. е. форме

$$\begin{aligned} a(0 \cdot x' + y')^2 + 2b(0 \cdot x' + y')(-x' + \delta y') + a'(-x' + \delta y')^2 &= \\ &= a'x'^2 + 2(-b + a'\delta)x'y' + (a + 2b\delta + a'\delta^2)y'^2 = \\ &= [e_1(0 \cdot x' + y') + e_2(-x' + \delta y')]^2 = \\ &= (-e_2x' + (e_1 + \delta e_2)y')^2, \end{aligned}$$



получаемой из нее преобразованием  $\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$ , соответствует репер, первый вектор  $e'_1$  которого равен вектору  $-e_2$ , обратному второму вектору  $e_2$  исходной формы  $(a, b, a')$ , и второй вектор  $e'_2$ , который равен  $e_1 + \delta e_2$ . Если, кроме того,  $\delta$  подобрано так, как указано выше, т. е. чтобы было  $2|b'| \leq a'$ , или, иначе,  $2||e'_1|| |e'_2| \cos \varphi' \leq$

$\leq |e'_1|^2$  или  $||e'_2| \cos \varphi'| \leq \frac{|e'_1|}{2}$ , то проекция второго вектора  $e'_2$  на первый  $e'_1$  по абсолютной величине меньше или равна половине длины  $|e'_1|$  первого вектора, т. е. конец второго вектора принадлежит полоске, ограниченной перпендикулярами, восставленными в серединах первого вектора  $e'_1$  и ему обратного вектора  $-e'_1$ .

Если, следовательно, переходить от заданной формы  $(a, b, a')$  к соседней с ней справа форме  $(a', b', a'')$ , от нее снова к соседней с ней справа форме  $(a'', b'', a''')$  и т. д., то в этом ряду форм, начиная с формы  $(a', b', a'')$ , будет каждый раз выполняться первое условие приведения  $2|B| \leq A$ . Но через конечное число шагов выполнится и второе условие приведения  $A \leq C$ , так как, если бы все время было  $a' > a'' > a'''$  и т. д., то получилось бы, что в данной решетке есть внутри круга радиуса  $\sqrt{a'}$ , описанного вокруг центра  $O$ , бесконечно много точек, все более и более близких к точке  $O$ , а этого быть не может.

Из этого геометрического рассуждения мы видим, таким образом, что, после конечного числа шагов алгоритма Гаусса соседних справа форм, мы от любой положительной формы  $(a, b, a')$  придем, в конце концов, к собственно эквивалентной ей приведенной форме.

Все полученные таким способом последующие реперы будут той же ориентации, как и исходный репер, т. е. формы, им соответствующие, будут собственно эквивалентны исходной форме.

То, что приведенная форма только одна, если у нее в обоих случаях имеют место неравенства, а не равенства, также легко показать геометрически.

3. *Теория приведения Гаусса для случая неспределенной двойничной квадратичной формы.* Случай  $D > 0$ , т. е. когда  $(a, b, a')$  — неопределенная двойничная квадратичная форма с вещественными коэффициентами, приводит к совсем другой теории. В этом случае форма разлагается на линейные множители с вещественными коэффициентами  $\xi_1, \xi_2, \eta_1, \eta_2$ , где  $\begin{vmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{vmatrix} \neq 0$ :

$$(a, b, a') = \rho (\xi_1 x + \xi_2 y) \frac{1}{\rho} (\eta_1 x + \eta_2 y),$$

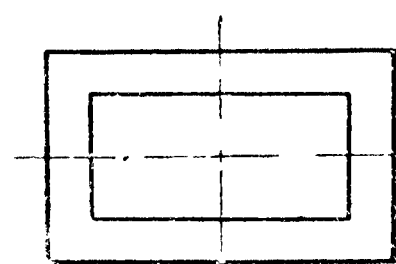
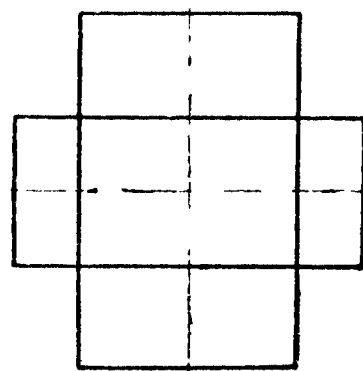
причем даже бесконечным числом разных способов, так как вещественный множитель  $\rho$  можно выбирать произвольно.

Зафиксируем как-нибудь множитель  $\rho$  и рассмотрим репер  $Oe_1e_2$ , векторы которого относительно некоторой выбранной декартовой координатной системы имеют координаты  $(\xi_1, \eta_1)$  и  $(\xi_2, \eta_2)$ .

Рассмотрим решетку, построенную на этом репере, и будем предполагать, что она не имеет, кроме начала, точек на координатных осях, что равносильно тому, что форма не разлагается на множители, пропорциональные рациональным. Неопределенную форму  $(A, B, C)$  Гаусс называет *приведенной*, если она удовлетворяет условиям:

$$\sqrt{D} - B < |A| < \sqrt{D} + B, \quad B > 0. \quad (2)$$

Если обратиться к рассмотренной сейчас геометрии таких форм и геометрически истолковать эти неравенства, то получается, что они обозначают следующее. Если называть параллелограмм, вершина которого — в рассматриваемой точке  $M$  (не лежащей на осях  $O\xi$  и  $O\eta$ ), центр которого — в начале и стороны параллельны координатным осям  $O\xi$  и  $O\eta$ , координатным параллелограммом точки  $M$ , то условия (2) обозначают то, что: 1) координатные параллелограммы концов первого и второго векторов репера, соответствующего форме  $(A, B, C)$ , скрещиваются, как на верхнем рисунке, а не охватывают один другой, как на нижнем рисунке, и 2) вдоль первой оси, т. е. оси  $O\xi$ , координатный параллелограмм второго вектора длиннее, чем первого.



Легко показать (это можно сделать и геометрически), что если от заданной неопределенной формы  $(a, b, a')$  переходить к соседней с ней справа, такой, что в  $b' = -b + a'\delta$  число  $\delta$  берется между  $\sqrt{D} - |a'|$  и  $\sqrt{D}$ , то через конечное число шагов придем к приведенной в этом смысле форме — собственно эквивалентной форме  $(a, b, a')$ .

Если же продолжать этот же алгоритм дальше, то будут получаться последовательные дальнейшие приведенные формы, соседние одна с другой, все более и более «длинные» вдоль оси  $O\xi$ .



Аналогично тому, как это сделал уже Лагранж, Гаусс показывает, что если коэффициенты формы — целые числа, то, хотя различных таких приведенных вдоль оси  $O\xi$  реперов бесконечно много, различных соответствующих им форм конечное число и они повторяются периодически. Геометрически это происходит от того, что решетка  $\Gamma$ , построенная на репере, соответствующем целочисленной определенной квадратичной форме, имеет гиперболические повороты в себя, т. е. имеет такие множители  $\rho$ , что если помножить все координаты  $\xi$  ее точек на  $\rho$  и разделить на  $\rho$  все координаты  $\eta$  ее точек, то решетка  $\Gamma$  совместится с собой.

Приведенные реперы, расположенные в одинаковых местах различных периодов, получаются один из другого таким автоморфизмом решетки  $\Gamma$ , и потому им соответствуют одинаковые квадратичные формы.

Для того чтобы решить задачу I, надо, таким образом, вычислить полный период приведенных форм, эквивалентных первой из заданных форм, и найти хотя бы одну приведенную форму, эквивалентную второй заданной форме, и тогда, если она встречается в периоде первой формы, то заданные формы эквивалентны, если нет, то — неэквивалентны.

В последних пп. 216—221 первой части пятого раздела Гаусс прилагает теорию двойничных форм, построенную им в предыдущих пп. 153—215 этого раздела, к решению в целых числах общего неопределенного уравнения 2-й степени с целыми коэффициентами:

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0.$$

Заключительный п. 222 первой части пятого раздела посвящен исторической справке о предшествующих «Арифметическим исследованиям» Гаусса работам Эйлера, Лагранжа и Лежандра, относящихся к тому же вопросу.

## 11. Вторая часть пятого раздела «Арифметических исследований».

### Композиция классов и композиция родов квадратичных форм

Вторая часть пятого раздела, озаглавленная «Дальнейшие исследования о формах» (пп. 223—265), содержит теорию композиции

классов целочисленных квадратичных двойничных форм данного определителя, всецело принадлежащую уже лично Гауссу.

То, что не все целочисленные двойничные квадратичные формы данного определителя эквиваленты и что они разбиваются на конечное число классов эквивалентных форм, было известно уже Лагранжу, но то, что эти классы можно компоновать друг с другом и что они образуют в смысле этой композиции конечную коммутативную (абелеву) группу, есть замечательное открытие Гаусса, оказавшееся как бы далекой и весьма нетривиальной разведкой в область теории алгебраических чисел, которая была совершена Гауссом задолго до того, как сама эта теория была окончательно построена. Трудно гадать, каков был путь, приведший Гаусса к открытию композиции классов, но, во всяком случае, предвидение ее важности не обмануло Гаусса.

1. *Основные определения — определение понятия «род».* Совокупность всех целочисленных двойничных квадратичных форм, собственно эквивалентных данной такой форме, образует *класс* (собственный) форм данного определителя. Как это непосредственно следует из теории приведения, в каждом классе форм данного определителя есть формы, все коэффициенты которых по абсолютной величине меньше данной функции от определителя; поэтому в случае форм с целыми коэффициентами число классов таких форм данного определителя конечно. В случае отрицательного определителя  $D = b^2 - ac < 0$ , т. е. когда форма определенная, достаточно рассматривать лишь положительные классы, т. е. классы форм, у которых  $D < 0$  и  $a > 0$ , так как отрицательные классы получаются из них просто изменением знаков всех коэффициентов всех форм на обратные.

Форму  $(a, b, c)$ , у которой  $a, b, c$  не имеют общего делителя, Гаусс называет *примитивной*, а если при этом  $a$  и  $c$  не оба четные, т. е. и числа  $a, 2b, c$ , не имеют общего делителя, то он называет форму *собственно примитивной*. Тогда и все ей эквивалентные формы тоже примитивные или собственно примитивные. Соответственно этому рассматриваются и классы примитивные и собственно примитивные. Два класса одного и того же определителя Гаусс относит к одному и тому же порядку (*ordo*), если  $(a, b, c)$  и  $(a', b', c')$  — формы этих классов, и как числа  $a, b, c$  и  $a', b', c'$  имеют один и тот же наибольший общий

делитель, так и числа  $a$ ,  $2b$ ,  $c$  и  $a'$ ,  $2b'$ ,  $c'$  имеют один и тот же наибольший общий делитель.

Наиболее важное значение имеет собственно примитивный порядок, так как непримитивные формы просто связаны с примитивными.

Совокупность классов собственно примитивного порядка данного определителя  $D$  Гаусс далее еще разделяет на *роды* (genere), относя в один и тот же род все те классы, формы которых имеют один и тот же *характер*. Под характером примитивной формы, или примитивного класса форм, так как у всех форм одного и того же класса, как легко показать, одинаковые характеры, Гаусс понимает следующее.

Пусть  $m$  — какой-нибудь простой делитель  $D$ , а в некоторых случаях надо еще рассмотреть числа  $m = 4$  и  $m = 8$ , и пусть число всех этих различных модулей  $m$  равно  $\lambda$ . Можно показать, что если  $m_i$  — один из этих  $\lambda$  модулей, то для всех чисел  $n$ , представляемых данной собственно примитивной формой определителя  $D$  и взаимно простых с  $2D$  для данного  $m_i$ , квадратичный характер  $\left(\frac{n}{m_i}\right)$  (символ Лежандра) имеет одно и то же значение. Выпишем эти квадратичные характеры, которые все равны  $+1$  или  $-1$ , для всех  $\lambda$  указанных модулей  $m_1, m_2, \dots, m_\lambda$ , взятых в каком-либо раз навсегда выбранном порядке; тогда для данной формы получается некоторая определенная последовательность  $\lambda$  чисел  $\pm 1$ . Эту последовательность Гаусс называет *характером* (Totalcharacter) рассматриваемой собственно примитивной формы определителя  $D$  или характером класса, ею представляемого. Так как число всех вообще возможных различных последовательностей, составленных из  $\lambda$  членов, равных  $+1$  или  $-1$ , равно  $2^\lambda$ , то число различных характеров форм данного определителя, а следовательно, и число родов никак не больше, чем  $2^\lambda$ . Однако неясно, всякая ли такая последовательность есть характер некоторого класса — а priori, может быть, что число родов и меньше?

Для того, чтобы дать ответ на глубокий вопрос о том, каково истинное число родов, Гаусс вводит особое исчисление, в котором элементами являются не числа, а классы форм.

2. *Композиция классов Гаусса и ее изложение по Дирихле.* Форма

$$F = AX^2 + 2BXY + CY^2$$

называется по Гауссу *компонированной* из форм

$$f = ax^2 + 2bxy + cy^2 \text{ и } f' = a'x'^2 + 2b'x'y' + c'y'^2,$$

если она переходит в их произведение при помощи целочисленной билинейной подстановки вида:

$$X = pxx' + p'xy' + p''yx' + p'''yy';$$

$$Y = qxx' + q'xy' + q''yx' + q'''yy',$$

где числа

$$\begin{vmatrix} p & p' \\ q & q' \end{vmatrix}, \begin{vmatrix} p & p'' \\ q & q'' \end{vmatrix}, \begin{vmatrix} p & p''' \\ q & q''' \end{vmatrix}, \begin{vmatrix} p' & p'' \\ q' & q'' \end{vmatrix}, \begin{vmatrix} p' & p''' \\ q' & q''' \end{vmatrix}, \begin{vmatrix} p'' & p''' \\ q'' & q''' \end{vmatrix}$$

не имеют общего им всем множителя, отличного от 1. При этом оказывается, что класс, к которому принадлежит форма  $F$ , вполне определяется тем, к каким классам принадлежат компонируемые формы  $f$  и  $f'$ .

Убедиться в возможности компонирования собственно примитивных форм одного и того же определителя проще не из изложения, данного самим Гауссом, а при помощи того упрощения этого изложения, которое предложил Дирихле. Наметим основные пункты этого упрощенного изложения теории Гаусса. Пусть  $f = ax^2 + 2bxy + cy^2$  — собственно примитивная форма, т. е. числа  $a, 2b, c$  не имеют общего им всем делителя, отличного от 1. Заметим прежде всего, что среди чисел, представляемых такой формой  $f$ , всегда существуют числа, взаимно простые с любым наперед заданным числом  $K$ . Действительно, если хотя бы один из крайних коэффициентов формы  $f$ , например  $a$ , не делится на простое число  $p$ , то для того, чтобы  $f$  не делилась на  $p$ , достаточно взять такие  $x$  и  $y$ , чтобы  $x$  не делилось на  $p$ , а  $y$  делилось на  $p$ . Если же оба крайние коэффициента  $f$  делятся на  $p$ , то средний  $2b$  уже не делится на  $p$ , так как форма собственно примитивная, и достаточно взять такие  $x$  и  $y$ , чтобы оба они не делились на  $p$ . Поэтому, если  $p_1, p_2, \dots, p_k$  — все различные простые делители числа  $K$ , то для того, чтобы  $f = ax^2 + 2bxy + cy^2$  была взаимно простой с  $K$ , достаточно так взять  $x$ , чтобы оно делилось на одни из этих простых чисел и не делилось на другие, и то же самое

сделать с  $y$ . При этом можно еще, очевидно, всегда выбрать  $x$  и  $y$  так, чтобы они были взаимно простыми.

Выберем теперь по форме из компонируемых классов, и пусть представитель второго из этих классов есть форма  $(a', b', c')$ . Возьмем такие взаимно простые числа  $x = \alpha$ ,  $y = \gamma$ , чтобы при подстановке их в представителя первого класса получалось число  $a$ , взаимно простое с числом  $a'$ , что, как мы сейчас видели, всегда можно сделать. Тогда, если взять такие  $\beta$  и  $\delta$ , чтобы было  $\alpha\delta - \beta\gamma = 1$ , то подстановка  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  переводит представителя первого класса в эквивалентную форму  $(a, b, c)$ , первый коэффициент которой  $a$  взаимно прост с первым коэффициентом  $a'$  представителя второго класса. Перейдем теперь еще от этих представителей  $(a, b, c)$  и  $(a', b', c')$  рассматриваемых классов с взаимно простыми  $a$  и  $a'$  далее к другим, им эквивалентным «параллельным» формам при помощи подстановок  $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$  и  $\begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix}$ . Эти формы будут иметь прежние первые коэффициенты  $a$  и  $a'$ , средние же их коэффициенты будут  $a\mu + b$  и  $a'\nu + b'$ . Подберем теперь так  $\mu$  и  $\nu$ , чтобы удовлетворялось следующее неопределенное уравнение 1-й степени:

$$a\mu + b = a'\nu + b',$$

что всегда можно сделать, так как числа  $a$  и  $a'$  взаимно простые. Обозначив  $a\mu + b$  через  $B$ , мы получим формы  $(a, B, \bar{c})$  и  $(a', B, \bar{c}')$ . Но определители этих форм равны, поэтому  $B^2 - a\bar{c} = B^2 - a'\bar{c}'$ , откуда, так как  $a$  и  $a'$  взаимно простые,  $\bar{c} = a'C$ ,  $\bar{c}' = aC$ . Выбранные нами, теперь уже окончательно, представители рассматриваемых нами классов имеют такой вид:

$$f = (a, B, a'C) \text{ и } f' = (a', B, aC).$$

Определители обеих этих форм равны  $B^2 - aa'C = d$ .

Разложим обе эти формы на линейные множители следующим образом:

$$f = \left( \sqrt{a} x + \frac{B + \sqrt{d}}{\sqrt{a}} y \right) \left( \sqrt{a} x + \frac{B - \sqrt{d}}{\sqrt{a}} y \right),$$

$$f' = \left( \sqrt{a'} x' + \frac{B + \sqrt{d}}{\sqrt{a'}} y' \right) \left( \sqrt{a'} x' + \frac{B - \sqrt{d}}{\sqrt{a'}} y' \right).$$

Перемножая первые множители, мы получим следующее тождество:

$$\begin{aligned} \left( \sqrt{a}x + \frac{B + \sqrt{d}}{\sqrt{a}}y \right) \left( \sqrt{a'}x' + \frac{B + \sqrt{d}}{\sqrt{a'}}y' \right) = \\ = \sqrt{aa'}(xx' - Cyy') + \frac{B + \sqrt{d}}{\sqrt{aa'}}(axy' + a'x'y + 2Byy'), \end{aligned} \quad (*)$$

а перемножая вторые множители, — аналогичное тождество, в котором только вместо  $\sqrt{d}$  стоит  $-\sqrt{d}$ . Перемножая оба эти тождества, мы получаем, что форма

$$F = (aa', B, C)$$

того же определителя  $B^2 - aa'C = d$  переходит в произведение форм  $f$  и  $f'$  при помощи билинейной подстановки

$$X = xx' - Cyy'; \quad Y = axy' + a'x'y + 2Byy'. \quad (1)$$

Коэффициенты ее

$$\begin{pmatrix} p & p' & p'' & p''' \\ q & q' & q'' & q''' \end{pmatrix}$$

суть

$$\begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a & a' & 2B \end{pmatrix},$$

определители  $\begin{vmatrix} -1 & 0 \\ 0 & a \end{vmatrix}$  и  $\begin{vmatrix} 1 & 0 \\ 0 & a' \end{vmatrix}$  взаимно простые.

Если были бы выбраны не эти специальные представители  $f$  и  $f'$  рассматриваемых классов (называемые Дирихле «*inige*» — «согласные»), а какие-либо произвольные, например, получаемые из них подстановками:

$$\begin{aligned} x &= \alpha\bar{x} + \beta\bar{y}, & x' &= \alpha'\bar{x}' + \beta'\bar{y}', \\ y &= \gamma\bar{x} + \delta\bar{y} & \text{и} & \quad y' = \gamma'\bar{x}' + \delta'\bar{y}', \end{aligned} \quad (2)$$

то результатом их композиции можно считать ту же форму  $F$ , но билинейная подстановка, при помощи которой она переходит

в произведение заданных форм, будет уже более сложная, а именно та, которая получается из билинейной подстановки (1) при помощи замены в ней  $x, y, x', y'$  по формулам (2).

3. *Связь с умножением решеток Клейна.* С той геометрической точки зрения, которую мы рассмотрели выше, теория Гаусса композиции классов принимает следующий вид.

Предположим для определенности, что определитель  $d$  положительный; если бы  $d$  было отрицательно, дальнейшее изложение было бы совершенно аналогичное. Решетка  $L$ , соответствующая форме  $f$ , построена (если  $d > 0$ ) на векторах  $(\sqrt{a}, \sqrt{a})$  и  $\left(\frac{B + \sqrt{d}}{\sqrt{a}}, \frac{B - \sqrt{d}}{\sqrt{a}}\right)$ , а решетка  $L'$ , соответствующая форме  $f'$ , построена на векторах  $(\sqrt{a'}, \sqrt{a'})$  и  $\left(\frac{B + \sqrt{d}}{\sqrt{a'}}, \frac{B - \sqrt{d}}{\sqrt{a'}}\right)$ . Тождество (\*)

показывает, что произведение точки решетки  $L$  с координатами  $x, y$ , относительно указанного ее основного репера, на точку решетки  $L'$  с координатами  $x', y'$ , относительно ее указанного основного репера, т. е. произведение любой точки решетки  $L$  на любую точку решетки  $L'$ , дает некоторую точку решетки  $L$ , соответствующей форме  $F$ , с координатами  $(xx' - Cyu', axu' + a'x'y + 2Byu')$ . Легко показать, что, соответственно выбирая точки решеток  $L$  и  $L'$  и складывая и вычитая их произведения, можно получить любую точку решетки  $L$ , т. е. что решетка  $L$  есть произведение в рассматриваемом нами на стр. 891 смысле решеток  $L$  и  $L'$ . Для этого, очевидно, достаточно показать, что концы  $M_1$  и  $M_2$  векторов основного репера решетки  $L$  могут быть получены следующим способом.

Точка  $M_1$  с первой координатой  $\sqrt{aa'}$ , очевидно, получается в результате умножения точек  $(1, 0)$  и  $(1, 0)$  решеток  $L$  и  $L'$ . Для того же чтобы получить точку  $M_2$  с первой координатой  $\frac{B + \sqrt{d}}{\sqrt{aa'}}$ , перемножим сначала точки  $(1, 0)$  и  $(0, 1)$  решеток  $L$  и  $L'$  и затем их точки  $(0, 1)$  и  $(1, 0)$ , тогда мы получим точки с первыми координатами  $\frac{B + \sqrt{d}}{\sqrt{a'}} \sqrt{a}$  и  $\frac{B + \sqrt{d}}{\sqrt{a}} \sqrt{a'}$  (вторые координаты будут из них получаться заменой  $\sqrt{d}$  на  $-\sqrt{d}$ ). Складывая эти точки  $z_1$  раз первую и еще  $z_2$  раз вторую, мы получим точку с первой

координатой:

$$\frac{B + \sqrt{d}}{\sqrt{a'}} \sqrt{a} z_1 + \frac{B + \sqrt{d}}{\sqrt{a}} \sqrt{a'} z_2 = \frac{B + \sqrt{d}}{\sqrt{aa'}} (az_1 + a'z_2),$$

а так как  $a$  и  $a'$  взаимно простые, то можно так выбрать  $z_1$  и  $z_2$ , чтобы было  $az_1 + a'z_2 = 1$ , и тогда мы получим точку  $M_2$ .

Итак, с геометрической точки зрения рассмотренная нами на стр. 917 композиция классов Гаусса есть не что иное, как умножение решеток, соответствующих этим классам, в том смысле, как умножение решеток было рассмотрено на стр. 891.

В своих лекциях «Избранные главы теории чисел»<sup>1</sup> Клейн говорит, что можно себя спросить, почему Гаусс вместо того, чтобы говорить об умножении решеток, говорит о композиции соответствующих им квадратичных форм. Клейн думает, что не невозможно, что уже при писании «Арифметических исследований» Гаусс знал о связи квадратичных форм с решетками, но не изложил вопроса так из каких-то своих личных соображений. А между тем, это изложение при помощи решеток дает больше, чем изложение при помощи форм, уже потому, «что отдельный линейный множитель, задающий решетку, учитывает абсолютную величину + азимут, а форма учитывает только абсолютную величину». «Композиция форм,—говорит Клейн,—есть, так сказать, лишь следствие, а не эквивалент теории умножения решеток». Идея рассмотрения решеток могла легче привести к связи с модулярными функциями. Кроме того, идея рассмотрения при композиции не самих форм, а линейных множителей форм, могла скорее привести к решению самого глубокого, связанного со всеми этими исследованиями арифметического вопроса, к построению теории делимости в полях алгебраических чисел.

4. *Связь с теорией квадратичных полей.* Какой же смысл имеет теория композиции двойничных квадратичных форм данного определителя, созданная Гауссом, с точки зрения теории алгебраических чисел? С той геометрической точки зрения, на которую мы стали в § 8 в изложении теории алгебраических чисел, дело обстоит так.

<sup>1</sup> F. K l e i n. Ausgewählte Kapiteln der Zahlentheorie, Teil II. Göttingen, 1907, стр. 133 (литограф.).



Пусть  $\Delta$  — целое положительное число, не делящееся на квадрат; тогда (см. § 8) кольцо  $\mathcal{O}$  всех целых точек квадратичного поля  $R(\sqrt{\Delta})$ , если  $\Delta \equiv 2$  или  $3 \pmod{4}$ , имеет базис  $(1, 1)$   $(\sqrt{\Delta}, -\sqrt{\Delta})$ , а если  $\Delta \equiv 1 \pmod{4}$ , имеет базис  $(1, 1)$   $\left(\frac{1+\sqrt{\Delta}}{2}, \frac{1-\sqrt{\Delta}}{2}\right)$ . Квадратичные формы, построенные на этих реперах, суть  $(x + \sqrt{\Delta}y) \times (x - \sqrt{\Delta}y) = x^2 - \Delta y^2$  и  $\left(x + \frac{1+\sqrt{\Delta}}{2}y\right) \left(x + \frac{1-\sqrt{\Delta}}{2}y\right) = x^2 + xy + \frac{1-\Delta}{4}y^2$ . Формы эти целочисленные, но вторая из них не имеет двойки в коэффициенте при  $xy$ . Но надо заметить, что теорию композиции форм Гаусса можно изложить и для целочисленных двойничных квадратичных форм вида  $ax^2 + bxy + cy^2$ , т. е. таких, у которых при  $xy$  стоит коэффициент  $b$ , а не  $2b$ , как у Гаусса. Определителем  $d$  формы тогда называется число  $b^2 - 4ac$ . Вся теория будет ровно такая же, как изложенная выше, только тождество (\*) надо будет заменить следующим:

$$\begin{aligned} \left(\sqrt{a}x + \frac{B + \sqrt{d}}{2\sqrt{a}}y\right) \left(\sqrt{a'}x' + \frac{B + \sqrt{d}}{2\sqrt{a'}}y'\right) = \\ = \sqrt{aa'}(xx' - cyy') + \frac{B + \sqrt{d}}{2\sqrt{aa'}}(axy' + a'x'y + Byy'). \end{aligned} \quad (**)$$

В случае, когда  $\Delta \equiv 2$  или  $3 \pmod{4}$ ,  $d$  будет равен  $4\Delta$ , а в случае  $\Delta \equiv 1 \pmod{4}$ ,  $d = 1 - 4 \cdot 1 \cdot \frac{1-\Delta}{4} = \Delta$ . Главный класс такого определителя  $d$  будет представляться как раз формой  $x^2 - \Delta y^2$  или соответственно формой  $x^2 + xy + \frac{1-\Delta}{4}y^2$ . Этим формам соответствует главная решетка  $\mathcal{O}$ . А остальным  $h - 1$  классам примитивных форм определителя  $d$  соответствуют побочные решетки  $\mathcal{O}'$ ,  $\mathcal{O}''$ , ...,  $\mathcal{O}^{(h-1)}$ , если для каждого из них соответственно выбрать множитель  $\rho$ . Выбор этих множителей, как показал Клейн, связан с рассмотрением базиса абелевой группы классов квадратичных форм определителя  $d$ . Композиции классов соответствует умножение решеток  $\mathcal{O}$ ,  $\mathcal{O}'$ ,  $\mathcal{O}''$ , ...,  $\mathcal{O}^{(h-1)}$  друг на друга.

Всякая точка всякой из так выбранных (в смысле выбора множителей  $\rho$ ) решеток  $\mathcal{O}$ ,  $\mathcal{O}'$ ,  $\mathcal{O}''$ , ...,  $\mathcal{O}^{(h-1)}$  разлагается однозначно в произведение простых точек этих решеток с точностью до

множителей единиц  $\varepsilon$ , которые все суть точки главной решетки  $\mathcal{O}$ , лежащие на гиперболах  $\xi\eta = \pm 1$ . От умножения на любую из них каждая из решеток  $\mathcal{O}, \mathcal{O}', \dots, \mathcal{O}^{(h-1)}$  переходит в себя, и каждая из форм соответствующего этой решетке класса целочисленно линейно унимодулярно преобразуется в себя.

С точки же зрения теории идеалов Дедекинда дело обстоит так. Если помножить решетку  $\mathcal{O}^{(k)}$  на какую-либо точку  $j$  решетки  $(\mathcal{O}^{(k)})^{-1}$ , то получается подрешетка  $\mathfrak{Z}$  главной решетки  $\mathcal{O}$ , которая есть идеал  $k$ -го класса решетки  $\mathcal{O}$ , и обратно. Квадратичная форма, соответствующая решетке  $\mathfrak{Z}$ , отличается от квадратичной формы определителя  $d$ , соответствующей решетке  $\mathcal{O}^{(k)}$ , целым рациональным множителем, который есть норма идеала  $\mathfrak{Z}$  в решетке  $\mathcal{O}$ , т. е. число, показывающее, во сколько раз площадь основного параллелограмма решетки  $\mathfrak{Z}$  больше, чем площадь основного параллелограмма решетки  $\mathcal{O}$ . Это число, очевидно, равно норме по отношению к осям  $O\xi\eta$  точки  $j$ , т. е. произведению  $\xi\eta$  ее координат.

Стоило Гауссу сделать в теории композиции форм еще один шаг дальше, а именно, разумно подобрав множитель  $\rho$  (т. е. правильно повернув решетки  $\mathcal{O}', \mathcal{O}'', \dots, \mathcal{O}^{(h-1)}$  по отношению к решетке  $\mathcal{O}$ ), начать умножать один на другой отдельные линейные множители квадратичных форм, лежащих в рассматриваемых классах (т. е. отдельные точки решеток  $\mathcal{O}, \mathcal{O}', \dots, \mathcal{O}^{(h-1)}$ ), как он обнаружил бы однозначность разложения и построил бы, задолго до Куммера, Дедекинда и Золотарева, арифметику полей алгебраических чисел.

Трудно сказать, что остановило Гаусса на этом пути. Быть может, одной из главных трудностей, которую, как кажется, так и не удалось преодолеть Гауссу, была для него теорема о базисе абелевой группы, без которой трудно сообразить, как выбирать множители  $\rho$  для форм, представляющих отдельные классы.

Классы форм данного определителя в смысле композиции, рассмотренной Гауссом, образуют абелеву группу. Главный класс является единицей этой группы. Два обратных класса, т. е. те, которые содержат формы  $(a, b, c)$  и  $(a, -b, c)$ , являются обратными элементами и т. д. Группа классов Гаусса была первой нетривиальной абелевой группой, которая обратила на себя внимание математиков. Хактеры классов, рассматриваемые Гауссом в его теории

родов, — первый нетривиальный пример характеров группы, причем даже не очень простой, так как характеры Гаусса — не числа, а последовательности чисел, правда, очень простых, только  $\pm 1$ . О той роли, которую сыграла теория композиции классов Гаусса в истории абелевых групп, мы скажем дальше (стр. 954), где будем рассматривать соображения Гаусса о регулярных и иррегулярных определителях, рассмотренных им в самом конце пятого раздела, в п. 306.

5. *Композиция родов и вывод неравенства  $g \leq 2^{\lambda-1}$ .* Вернемся теперь снова к вопросу о числе родов целочисленных собственно примитивных двойничных квадратичных форм данного определителя  $D$ , т. е. к той глубокой задаче, для решения которой Гаусс создал свою композицию классов.

В п. 246 Гаусс рассматривает композицию родов, а именно он отмечает, что при композиции классов характеры этих классов перемножаются, а следовательно, род, к которому принадлежит класс, являющийся результатом композиции двух каких-либо классов, вполне определяется тем, в каких родах лежат эти классы, т. е., как теперь бы сказали, характеры классов дают обычным своим умножением гомоморфное представление группы классов.

В п. 252 Гаусс, опираясь на этот результат, естественно приходит к тому, что в каждом роде одно и то же число классов. Обозначая поэтому, как ранее, число классов через  $h$ , число родов — через  $\gamma$ , а число классов в роде — через  $g$ , Гаусс получает  $h = g\gamma$ . Гаусс называет *двусторонними* (ambiges) классами те классы, квадраты которых (в смысле композиции классов) дают главный класс.

В п. 257 и следующих Гаусс доказывает, что число двусторонних классов равно  $\frac{1}{2}\chi$ , где  $\chi = 2^{\lambda}$  есть число всех возможных различных последовательностей, состоящих из  $\lambda$  чисел, равных  $\pm 1$ . Далее, опять, как бы мы сейчас сказали, просто из групповых соображений, Гаусс показывает, что если обозначить число двусторонних классов через  $\alpha$ , а число тех классов, которые суть квадраты некоторых классов, через  $\delta$ , то  $h = \alpha\delta$ . Но все классы, которые суть квадраты некоторых классов, принадлежат к главному роду, так как характер каждого из таких классов есть квадрат

характера того класса, квадратом которого он является, т. е. состоит только из  $+1$ , а это характер главного рода. Поэтому  $\delta \leq g$ . Учитывая это неравенство и то, что  $h = g\gamma$  и  $h = \alpha\delta$ , Гаусс в п. 261 получает, что  $\gamma \leq \alpha$ , т. е. число родов не более, чем  $2^{\lambda-1}$ . Другими словами, по крайней мере половина из всех возможных последовательностей из  $\lambda$  чисел  $\pm 1$  не представляет собой характера никакого собственного примитивного класса определителя  $D$ .

В п. 262 Гаусс из этого неравенства для числа родов получает новое, второе, доказательство квадратичного закона взаимности, которое некоторые математики считают наиболее глубоким из всех, данных Гауссом.

Итак, число родов  $\gamma \leq 2^{\lambda-1}$ , но сколько именно родов — остается и на этом месте «Арифметических исследований» все же невыясненным. Для выяснения этого важного вопроса Гаусс употребляет новое средство — теорию тройничных целочисленных квадратичных форм.

## 12. Третья часть пятого раздела «Арифметических исследований».

### Отступление о тройничных формах

Эта часть пятого раздела «Арифметических исследований» озаглавлена: «Отступление, содержащее исследование о тройничных формах» (пп. 266—285).

В этом «Отступлении» Гаусс рассматривает теорию форм

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx',$$

которые он обозначает  $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$ , где  $a, a', a'', b, b', b''$  — целые рациональные числа.

Число

$$\Delta = ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2b'bb''$$

Гаусс называет *определителем* такой формы и предполагает его неравным нулю.

В этой части пятого раздела Гаусс кладет начало обширной области исследований, посвященных арифметической теории квадратичных форм от многих переменных, в которой впоследствии дали важ-

ные результаты Зеебер, Эйзенштейн, Дирихле, Арнольд Мейер, Зеллинг, Коркин и Золотарев, Смит, Минковский, Вороной, Венков, Хассе, Зигель и др. Сам Гаусс построил только самые элементы этой теории, необходимые ему для решения вопроса о числе родов двойничных квадратичных форм.

1. Рассмотрение Гауссом параллельно с данной тройничной формой ей союзной формы, геометрический смысл этого и значение для кристаллографии. Рядом с заданной тройничной формой  $f$  Гаусс рассматривает всегда так называемую союзную с ней форму (forma adjuncta)

$$F = Ax^2 + A'x'^2 + A''x''^2 + 2Bx'x'' + 2B'x''x + 2B''xx',$$

где

$$A = b^2 - a'a'', \quad A' = b'^2 - aa'', \quad A'' = b''^2 - aa';$$

$$B = ab - b'b'', \quad B' = a'b' - bb'', \quad B'' = a''b'' - bb'.$$

Сделаем в этом месте геометрическое замечание. Если форма  $f$  положительная, т. е. все числа, ею представляемые, положительны, то, как нетрудно показать,  $f = (xe_1 + x'e_2 + x''e_3)^2$ , т. е. равна скалярному квадрату линейного векторного выражения, причем если  $\Delta \neq 0$ , то векторы  $e_1, e_2, e_3$  не компланарны. Трехмерная «решетка»  $\Gamma$  всех точек, имеющих целые рациональные координаты относительно репера  $Oe_1e_2e_3$  (совершенно подобно тому, как в случае двойничной квадратичной формы двумерная решетка, построенная на репере  $Oe_1e_2$ , ей соответствующем), связана с формой  $f$  так, что эквивалентным с  $f$  формам, т. е. формам, получаемым из  $f$  линейными подстановками

$$\left. \begin{aligned} x &= \alpha\bar{x} + \beta\bar{x}' + \gamma\bar{x}'', \\ x' &= \alpha'\bar{x} + \beta'\bar{x}' + \gamma'\bar{x}'', \\ x'' &= \alpha''\bar{x} + \beta''\bar{x}' + \gamma''\bar{x}'' \end{aligned} \right\}$$

с целыми рациональными коэффициентами и определителем  $\pm 1$ , соответствуют другие основные реперы этой же решетки  $\Gamma$ , т. е. решетке соответствует в этом смысле класс эквивалентных форм, а отдельным формам класса — отдельные основные реперы решетки.

Репером, союзным (= взаимным = полярным = обратным) к данному реперу  $Oe_1e_2e_3$ , называется репер  $Oe_1^*e_2^*e_3^*$ , такой, что

скалярное произведение  $(xe_1 + x'e_2 + x''e_3)(x^*e_1^* + x'^*e_2^* + x''^*e_3^*)$  равно просто  $xx^* + x'x'^* + x''x''^*$ , т. е. такой репер, что

$$e_1^* = \frac{[e_2e_3]}{(e_1[e_2e_3])}, e_2^* = \frac{[e_3e_1]}{(e_2[e_3e_1])}, e_3^* = \frac{[e_1e_2]}{(e_3[e_1e_2])},$$

где  $[ \ ]$  обозначают векторное, а  $( \ )$  — скалярное произведение.

Решетка  $\Gamma^*$ , построенная на союзном репере, называется *союзной* с решеткой  $\Gamma$ . Важнейшее для кристаллографии свойство союзной решетки состоит в том, что всякий вектор союзной решетки  $\Gamma^*$  перпендикулярен к некоторой плоской сетке (т. е. двумерной подрешетке) заданной решетки  $\Gamma$  и по длине равен площади ее основного параллелограмма, и обратно. Это обстоятельство позволяет свести изучение плоских сеток решетки  $\Gamma$  параллельно-переносной повторяемости кристалла (которые играют существенную роль как в вопросах о плоских гранях кристалла, параллельных наиболее густым таким сеткам, так и в вопросах рентгеновского, электронного и нейтронного анализа структуры кристаллов) к изучению векторов взаимной решетки  $\Gamma^*$ .

Рассмотрение Гауссом союзной формы было очень важным шагом, так как эта форма или, скорее, связанная с ней геометрическая концепция союзной (=взаимной) решетки впоследствии стала играть (и играет сейчас) большую роль в практической кристаллографии. Надо, однако, сказать, что рассмотрение трехмерного репера, взаимного с данным, к которому все сводится, было сделано гораздо раньше Гаусса Лагранжем в его статье «О треугольных пирамидах» \* в 1773 г., в которой Лагранж изучал разные геометрические свойства тетраэдров, исходя из задания тетраэдра, имеющего одну вершину в начале координат, девятью координатами трех других его вершин. Эта статья Лагранжа, по-видимому, осталась мало замеченной, и француз кристаллограф Браве, первый введший взаимную решетку в кристаллографию, ссылается на Гаусса.

Рассмотрение Гауссом далее теории представления тройничной формой  $f$  двойничной квадратичной формы  $\varphi$  (п. 280) связано как

---

\* Solutions analytiques de quelques problèmes sur les pyramides triangulaires, 1773 (Oeuvres, t. III).

раз с этой взаимностью, в силу которой всякому такому представлению соответствует представление определителя  $D$  этой формы  $\varphi$ , союзной с  $f$  формой  $F$ .

2. Как Гаусс решает вопрос о положительности тройничной квадратичной формы. Отметим, между прочим, как Гаусс в п. 271 решает вопрос о том, является ли заданная тройничная квадратичная форма  $f$  положительной определенной или нет. Помножив  $f$  на  $a$ , Гаусс получает форму

$$g = (ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - Ax''^2,$$

а помножив форму  $g$  еще на  $A'$ , он получает форму

$$h = A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + a\Delta x'^2$$

и говорит: если  $A'$  и  $a\Delta$  отрицательны, то  $h$  представляет только отрицательные числа, почему  $f$  тогда представляет только числа, знак которых обратен знаку  $aA'$ , т. е. числа того же знака, как  $a$ . Таким образом, в этом случае форма  $f$  определенная и притом положительная, если  $a > 0$ , и отрицательная, если  $a < 0$ . Если же числа  $a\Delta$  и  $A'$  положительные или одно из них положительно, а другое отрицательно (но оба не равны нулю), то легко видеть, что соответственным подбором  $x, x', x''$  форма  $h$  может быть сделана как положительной, так и отрицательной, т. е. форма  $f$  неопределенная. Далее отдельно еще исследуются случаи  $A' = 0, a \neq 0$  и  $a = 0$  и доказывается, что в этих случаях форма  $f$  неопределенная. Из всего этого Гаусс выводит следствие, что у положительной формы числа  $A, A', A'', a\Delta, a'\Delta, a''\Delta$  отрицательны, числа  $a, a', a''$  положительны и число  $\Delta$  отрицательно.

Любопытно, что Гаусс не задается целью найти систему независимых необходимых и достаточных условий положительности формы  $f$ . Сейчас мы знаем, что эти условия следующие:

$$\begin{vmatrix} a & b'' & b' \\ b'' & a' & b \\ b' & b & a'' \end{vmatrix} > 0, \quad \begin{vmatrix} a & b'' \\ b'' & a' \end{vmatrix} > 0, \quad a > 0,$$

или в обозначениях Гаусса:  $\Delta < 0, A'' < 0, a > 0$ . Гаусс даже не отмечает, что девять выведенных им условий не только необходимы,

но и достаточны. То же самое замечание надо сделать относительно рассмотренных на стр. 910 и 913 условий приведения двойничной положительной и неопределенной квадратичной формы. Как в тех, так и в других условиях у Гаусса к выписанным нами прибавлено еще по одному лишнему условию, которое есть следствие остальных.

3. *Доказательство Гауссом конечности числа классов целочисленных тройничных квадратичных форм при помощи теории приведения таких форм.* В пп. 272—275 Гаусс дает способ приведения тройничной квадратичной формы, причем способ такой, который одновременно годится как для случая, когда форма  $f$  определенная, так и для случая, когда она неопределенная. В силу уже этого обстоятельства условия приведения Гаусса для положительной тройничной квадратичной формы не приводят к одной приведенной форме (как это имеет место у Зеебера). Они лишь таковы, что абсолютные величины всех коэффициентов приведенной формы, как в случае, когда форма определенная, так и в случае, когда она неопределенная, могут быть ограничены в зависимости от определения  $\Delta$  формы  $f$ . Поэтому, если коэффициенты  $a, a', a'', b, b', b''$  формы  $f$  целые рациональные, число различных таких приведенных форм определителя  $\Delta$  конечно. Отсюда в п. 276 получается теорема о том, что, подобно тому, как для двойничных целочисленных квадратичных форм, число классов целочисленных тройничных квадратичных форм данного определителя  $\Delta$  конечно. Итак, эту основную теорему условия приведения Гаусса дают. Но условия Гаусса приведения тройничных квадратичных форм в том смысле несовершенны, что если даны две эквивалентные между собой такие формы  $f$  и  $f'$ , то может быть, что ни одна форма, приведенная в смысле Гаусса, эквивалентная второй из них, не будет совпадать ни с одной из форм, приведенных в смысле Гаусса, эквивалентных первой. Таким образом, эта теория приведения Гаусса тройничных квадратичных форм не дает возможности решить вопрос об эквивалентности двух таких форм  $f$  и  $f'$ .

4. *Сведение Гауссом представления чисел тройничной квадратичной формы к задаче эквивалентности двух таких форм.* В п. 280 Гаусс начинает рассматривать теорию представления тройничной квадратичной формой  $f$  определителя  $\Delta$  двойничной формы

$$\varphi = pt^2 + 2qtu + ru^2$$



определителя  $D$ , если положить в форме  $f$

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u.$$

Легко убедиться, что в этом случае форма  $F$ , союзная с  $f$ , представляет число  $D$ , если положить в ней

$$X = m'n'' - m''n', \quad X' = m''n - mn'', \quad X'' = mn' - m'n.$$

Наоборот, оказывается, что всякое представление  $X, X', X''$  числа  $D$  союзной формой  $F$  таким образом получается из некоторого представления некоторой двойничной формы  $\varphi$  определителя  $D$  формой  $f$ . Геометрический смысл этого обстоятельства мы выяснили выше на стр. 928.

Отсюда следует, что решение задачи: найти все собственные представления числа  $D$  формой  $F$  сводится к тому, чтобы выписать представителей всех классов целочисленных двойничных квадратичных форм определителя  $D$  и найти все собственные представления этих представителей формой  $f$ , если они есть. Все эти представления и дадут все представления числа  $D$  формой  $F$ .

В п. 283 предлагается следующий способ находить все собственные представления двойничной формы

$$\varphi = pt^2 + 2qtu + ru^2$$

определителя  $D$  тройничной формой  $f$  определителя  $\Delta$ .

Пусть  $B$  и  $B'$  — такие целые рациональные числа, что  $B^2 \equiv a$ ,  $BB' \equiv b$ ,  $B'^2 \equiv c \pmod{D}$ ; тогда линейную форму  $Bx + B'y$  Гаусс называет значением  $\sqrt{ax^2 + 2bxy + cy^2} \pmod{D}$ . Гаусс показывает, что всякое собственное представление формы  $\varphi$  формой  $f$  принадлежит к некоторому «значению»  $(B, B')$ , и выводит следующее правило для нахождения всех собственных представлений формы  $\varphi$  формой  $f$ .

Найти все различные «значения»  $\sqrt{\Delta(pt^2 + 2qtu + ru^2)} \pmod{D}$ . Если два таких «значения» обратны по знаку, надо брать только одно из них. Чтобы найти все собственные представления формы  $\varphi$  формой  $f$ , принадлежащие к данному «значению»  $(B, B')$ , одно найти тройничную форму  $g = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$  определителя  $\Delta$ , в ко-

торой  $a = p$ ,  $b'' = g$ ,  $a' = r$ ,  $ab - b'b'' = B$ ,  $a'b' - bb'' = B'$ , откуда уже найдутся  $a''$ ,  $b$ ,  $b'$ , но, вообще говоря, в виде дробных чисел. Если либо один из коэффициентов  $a''$ ,  $b$ ,  $b'$  выйдет нецелым, либо формы  $f$  и  $g$  не будут эквивалентны, то представлений формы  $\varphi$  формой  $f$ , соответствующих «значению»  $(B, B')$ , нет. Если же  $a''$ ,  $b$ ,  $b'$  выйдут целые и формы  $f$  и  $g$  эквивалентны, то каждое преобразование

$$\begin{array}{ccc} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{array}$$

формы  $f$  в форму  $g$  дает такое представление:

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u,$$

и обратно.

В силу вышеописанной связи между представлениями числа  $D$  формой  $F$  и представлениями двойничной формы  $\varphi$  формой  $f$  задача о представлении чисел тройничной целочисленной квадратичной формой сводится к задаче установления эквивалентности двух тройничных целочисленных квадратичных форм  $f$  и  $g$ , и в случае, если они эквивалентны, к нахождению всех подстановок, при помощи которых одна из них переходит в другую, совершенно аналогично тому, как это было в вопросе о представлении чисел двойничной целочисленной квадратичной формой.

5. *Недостаток теории приведения Гаусса тройничных квадратичных форм.* К сожалению, теория приведения Гаусса тройничных квадратичных форм, как это было указано выше, не дает возможности решить вопрос об эквивалентности двух целочисленных тройничных квадратичных форм  $f$  и  $g$ , а потому и задача представления чисел такой формой также не получает у Гаусса полного решения. Сам Гаусс говорит об этом в п. 285 следующее: «Относительно вопросов, которые образуют третью из поставленных нами проблем (к которой в предыдущем сведены обе первые проблемы), а именно, если заданы две тройничные формы с одним и тем же определителем, узнать, эквивалентны они или нет, и в первом случае найти все преобразования одной из них в другую, мы можем в этом месте сказать только немного, так как полное решение, которое мы указали для анало-

гичной проблемы в случае двойничных форм, здесь наталкивается на еще бóльшие трудности. Поэтому мы ограничим наше исследование некоторыми специальными случаями, ради которых мы главным образом предприняли это отступление (т. е. изложение теории тройничных форм — Б. Д.) от нашего основного предмета (т. е. от исследования теории двойничных квадратичных форм — Б. Д.)».

Еще раньше в п. 277, посвященном теории приведения тройничных квадратичных форм, Гаусс прямым вычислением показал, что всякая целочисленная неопределенная тройничная квадратичная форма определителя  $\Delta = +1$  может быть преобразована в форму  $x^2 - 2yz$ . Собственно, этот частный результат о том, что существует только один класс целочисленных тройничных неопределенных квадратичных форм с определителем  $\Delta = +1$  только и нужен Гауссу дальше из всей теории приведения тройничных форм.

6. Работа Зеебера 1831 г. о положительных тройничных квадратичных формах, аннотация Гаусса к ней и работа Дирихле 1841 г. Возможно, как мы это уже выше говорили, что геометрическое толкование теории квадратичных форм было уже близко Гауссу в то время, когда он писал «Арифметические исследования», хотя в них он нигде ни слова об этом не упоминает. Опубликовано это геометрическое толкование было Гауссом гораздо позже, в 1831 г., в его аннотации (Anzeige) к работе Зеебера о приведении положительных тройничных квадратичных форм\*.

В первой статье Зеебер рассматривает разбиение пространства на одинаковые параллелепипедальные молекулы, причем рассмотрение квадрата расстояния между вершинами таких параллелепипедов, образующими некоторую решетку  $\Gamma$ , приводит его к геометрическому смыслу положительной тройничной квадратичной формы. В обширной (132 стр.) второй работе Зеебер решает задачу приведения положительных тройничных квадратичных форм так, что в каждом классе оказывается, как у Гаусса в случае положительных двойничных форм, лишь одна приведенная в его смысле форма. Зеебер говорит,

---

\* S e e b e r. Versuch einer Erklärung des inneren Baues der festen Körper, 1824; Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen, 1831.

что его привела к этому решению предыдущая кристаллографическая работа. Таким образом, «Теория положительных тройничных квадратичных форм,— говорит Зеебер,— становится полезным или даже необходимым орудием кристаллографии». Интересно отметить, как в этом месте при создании теории переплетаются между собой вопросы теории чисел и кристаллографии.

В «Anzeige» к работе Зеебера Гаусс дает доказательство неравенства  $aa'a'' < 2\Delta$ , которому удовлетворяет приведенная по Зееберу форма. Это неравенство Зеебер нашел лишь эмпирически, на примерах, но не дал его общего доказательства, а доказал лишь, что  $aa'a'' < 3\Delta$ . Доказательство, которое предлагает Гаусс, получается из одного арифметического тождества. Впоследствии Коркиным и Золотаревым, Минковским и др. это неравенство было обобщено на случай положительных квадратичных форм от  $n$  переменных. Оно означает, что в каждой решетке есть основной репер, мало отличающийся от ортогонального». Остальная часть «Anzeige» Гаусса посвящена изложению геометризации двойничных и тройничных квадратичных форм (положительных), рассмотренной нами выше на стр. 926. В самом конце Гаусс замечает, что положительная тройничная квадратичная форма будет приведенной по Зееберу тогда, когда параллелепипед, построенный на соответствующем ей репере, такой, что каждое из его ребер не длиннее диагоналей тех граней, которым они принадлежат, и не длиннее внутренних его диагоналей. Указанное же выше неравенство Зеебера, замечает Гаусс, означает просто то, что объем такого параллелепипеда, помноженный на  $\sqrt{2}$ , не меньше, чем объем прямоугольного параллелепипеда с такими же ребрами.

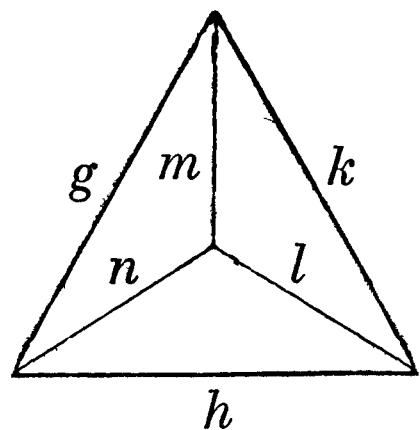
Простое и весьма изящное геометрическое доказательство существования в каждой трехмерной решетке основного параллелепипеда, удовлетворяющего условиям приведения Зеебера, дал в 1850 г. Дирихле в работе «*Über die Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen*» (Crelle, 40, 1850). Эта работа Дирихле, опубликованная еще задолго до смерти Гаусса, была, по нашему мнению, первой в истории математики серьезной работой по геометрии чисел. В этой работе Дирихле впервые вводит тот шестиугольник, который сейчас принято называть *областью Дирихле* точка

решетки. Для других целей этот шестиугольник позже рассматривал Эрмит в работе об обобщении непрерывных дробей, предложенном Чебышевым. Общую теорию таких областей для решеток любого числа измерений дал в своей знаменитой работе «*Recherches sur les paralléloèdres primitifs*» (1908—1909) Г. Ф. Вороной.

7. *Способ задавать трехмерную решетку.* Скажем еще несколько слов о том, как задают решетку. Кристаллографы обычно задавали решетку длинами ребер и величинами углов какого-нибудь ее основного репера. Это во всех смыслах неоднородное задание — даже размерность выбранных параметров неодинакова.

Гаусс задавал основной репер решетки квадратами длин его ребер  $a, a', a''$  и скалярными произведениями его ребер друг на друга  $b, b', b''$ , и записывал это так:  $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$ . Задание Гаусса однородно в смысле размерности выбранных параметров.

Первый, кто после Гаусса сделал дальнейший шаг в вопросе о задании решетки, был Зеллинг (Selling). В работе 1873 г. «*Über die binären und ternären quadratischen Formen*» (Crelle, 74, 1873) Зеллинг предложил кроме векторов  $e_1, e_2, e_3$  репера всегда рассматривать еще четвертый вектор  $e_4 = -e_1 - e_2 - e_3$ . Задание Зеллинга в некотором смысле более однородно, чем задание Гаусса. Численно такой четырехвекторник Зеллинг задает шестью параметрами — попарными скалярными произведениями его векторов друг на друга  $(e_2e_3), (e_3e_1), (e_1e_2), (e_1e_4), (e_2e_4), (e_3e_4)$ , обозначая их  $g, h, k, l, m, n$  — и записывает это так:  $\begin{pmatrix} g, h, k \\ l, m, n \end{pmatrix}$ . Своей записью Зеллинг снова уничтожает достигнутую им симметрию.



Еще более совершенна запись решетки, предложенная в работе «*Neue Begründung der geometrischen Kristallographie*» (Zeitschr. für Kristallographie, 1932) автором настоящей статьи, при помощи символа, представляющего

пространственный тетраэдр, на ребрах которого написаны параметры Зеллинга. Только в этой записи непосредственно по приведенному (по Зеллингу) символу обнаруживаются все симметрии решетки (группа ее «поворотов» в себя, тип ее параллелепипеда Браве и т. д.).

8. 7 голоэдрих решеток и 32 кристаллографических класса, 14 решеток Браве и 73 арифметических класса кристаллов. Кристаллографы много занимались вопросом о тех группах «вращений» (вращений вокруг точки решетки и таких же вращений плюс отражение в плоскости, проходящей через эту точку), при которых трехмерная решетка  $\Gamma$  совмещается с собой. Таких групп 7 — это так называемые голоэдрии. Если рассмотреть и все их подгруппы, то получается 32 группы, называемые *кристаллографическими классами*. Каждая из этих подгрупп причисляется к наименьшей из тех голоэдрих, которых она есть подгруппа. Так получается разбиение 32 классов на 7 сингоний. Кристаллограф Браве в своей знаменитой работе 1851 г. «*Sur les points distribués régulièrement sur le plan et dans l'espace*» вывел, кроме того, все возможные существенно различные решетки, имеющие ту или иную голоэдрию: три — для кубической голоэдрии, одну — для ромбоидальной, две — для квадратной (= тетрагональной) голоэдрии, четыре — для ортогональной (= ромбической) голоэдрии, две — для моноклинной, одну — для триклинной и одну — для гексагональной голоэдрии — всего 14 типов решеток Браве. *Параллелепипедом Браве* данной решетки  $\Gamma$  называется наименьший из параллелепипедов решетки  $\Gamma$  (т. е. параллелепипедов, вершинами которых являются точки решетки  $\Gamma$ ), вообще говоря, уже не основной, который (как тело) имеет ту же группу «поворотов» в себя, какую имеет сама решетка  $\Gamma$ , или наименьший из прямоугольных таких параллелепипедов, если такие в решетке есть. Гексагональная решетка не имеет параллелепипеда Браве, так как никакой параллелепипед не может иметь шестерной оси симметрии.

Совокупность всех преобразований данной положительной тройничной квадратичной формы в себя это не что иное, как голоэдриа решетки, т. е. группа всех ортогональных преобразований решетки в себя, оставляющих одну ее точку на месте, записанных целочисленными унимодулярными (вообще говоря, неортогональными) матрицами по отношению к некоторому основному реперу решетки. Если преобразовать все матрицы такой группы матриц одной и той же произвольной унимодулярной матрицей, то мы получим так называемую эквивалентную запись голоэдрии решетки, т. е. запись ее голо-

эдри по отношению к некоторому другому основному реперу решетки. Если считать различными такие группы целочисленных матриц, записывающих голоэдрию решетки, которые не эквивалентны в этом смысле, то различных таких групп оказывается 14, каждая соответствует своей решетке Браве. Если же взять и все их подгруппы, различные в этом же смысле, то получится всего 73 кристаллографических класса. Эту точку зрения проводит сейчас школа известного швейцарского кристаллографа Ниггли.

В этом смысле 7 голоэдрий можно называть *геометрическими голоэдриями*, а 14 решеток Браве — *арифметическими голоэдриями*; 32 кристаллографических класса — *геометрическими классами*, а введенные сейчас 73 кристаллографических класса — *арифметическими классами*.

9. *Теория приведения положительных квадратичных форм с тремя и с  $n$  переменными.* Что касается дальнейшей истории теории приведения целочисленных тройничных квадратичных форм, то о случае определенных форм мы уже говорили, для них весь вопрос был в высшей степени удовлетворительным образом решен Зеебером. Дополнение к нему оставалось сделать лишь в отношении вопроса о подстановках, преобразующих данную форму в себя; теорию таких подстановок разработали Эйзенштейн и Борисов. Затем Зеллинг в упомянутой работе 1873 г., исходя из своего четырехвекторника, дал новую, отличающуюся от зееберовой, теорию приведения тройничных положительных форм. Автор настоящей статьи в упомянутой выше работе 1932 г. связал эту теорию приведения положительной тройничной квадратичной формы с теорией области Вороного решетки, и довел ее до завершающей таблицы 24 сортов решеток, законченно решающей весь этот вопрос, так что результат стал удобен для использования в кристаллографии\*.

Обобщение теории приведения Зеллинга на положительные квадратичные формы с четырьмя переменными дал Шарв (Charve). Первый, кто показал, что можно и для положительной квадратичной формы с  $n$  переменными выделить при помощи (может быть, и беско-

---

\* Этот метод автора приняли сейчас в международном справочнике по структурному анализу кристаллов (1952). Им перевычислены почти все известные до сих пор структуры; см. справочник Donnay Crystal data, 1956.



нечного числа) линейных неравенств область изменения их коэффициентов (основную область приведения) такую, что: 1) никакие две формы из этой области неэквивалентны и 2) любая положительная квадратичная форма с  $n$  переменными имеет себе эквивалентную в этой области,— был Эрмит (Hermite); то же, что можно выделить такую область при помощи конечного числа линейных неравенств, показал в замечательной работе «*Discontinuitätsbereich für arithmetische Äquivalenz*» (Ges. Abh., Bd. II) Минковский. Исходя из идей Вороного, Б. А. Венков показал в работе «О приведении положительных квадратичных форм» \*, что если  $n > 2$ , то существует континуум различных разбиений области положительных квадратичных форм с  $n$  переменными на фундаментальные области приведения, каждая из которых задается конечным числом неравенств, причем разбиение Минковского является лишь одним из таких разбиений. Для получения разбиений Венкова надо рассмотреть произвольную положительную форму и все ей эквивалентные  $\varphi, \varphi', \varphi'', \dots$ . Разбиение Венкова получается, если рассмотреть пирамиды, на которые разбивается в пространстве коэффициентов конус положительных форм, каждая из которых является областью Вороного соответственной формы  $\varphi^{(i)}$  в смысле мероопределения Вороного. Если  $n > 2$  и исходную форму  $\varphi$  непрерывно изменять, разбиение это тоже непрерывно изменяется. В противоположность этому, как заметил еще раньше автор этих строк, для  $n = 2$  существует только одно такое разбиение, так как при изменении  $\varphi$  все стенки разбиения Венкова сохраняются.

10. *Теория приведения неопределенных тройничных квадратичных форм и квадратичных форм с  $n$  переменными сигнатуры  $n - 2$ .* Что касается теории приведения неопределенных квадратичных форм, то она гораздо труднее. Для произвольного  $n$  и произвольной сигнатуры она не завершена еще и теперь. Для неопределенных тройничных форм теория эта сейчас совершенно закончена. Наиболее далеко идущий результат принадлежит здесь также Б. А. Венкову. Поясним, в чем дело. В случае определенной двойничной или тройничной квадратичной формы существует одна и только одна эквивалентная ей приведенная (в случае двойничной приведенная по Гауссу, а в случае тройничной приведенная по Зееберу) форма и только в том

\* «Известия АН СССР», № 4, 1940.



случае, если решетка имеет симметрии, то — несколько (конечное число) таких приведенных форм, но они все могут быть легко найдены. В силу этого в случае положительной двойничной или тройничной квадратичной формы всегда можно узнать, эквивалентна ли она другой заданной такой форме, т. е. являются ли реперы, соответствующие этим формам, разными реперами одной и той же решетки или нет; все равно, целые или любые действительные числа — коэффициенты этих форм.

Совсем иные обстоятельства характеризуют неопределенные формы.

Если задана неопределенная двойничная квадратичная форма  $(a, b, c)$ , то указанным на стр. 913 алгоритмом можно посредством конечного числа шагов прийти от нее к эквивалентной ей приведенной (в смысле стр. 913) форме и далее находить тем же алгоритмом последовательные следующие формы цепочки приведенных форм, эквивалентных заданной форме. Если коэффициенты  $a, b, c$  не пропорциональны целым числам, то все формы этой цепочки будут различные, если же  $a, b, c$  целые (или пропорциональны целым числам), то различных форм в этой (бесконечной в обе стороны) цепочке будет лишь конечное число — они будут периодически повторяться. Дело в том, что если  $a, b, c$  пропорциональны целым числам, то решетка  $\Gamma$ , построенная на репере, соответствующем форме  $\varphi = (a, b, c)$ , будет при ее гиперболическом «вращении» относительно асимптот  $O\xi, O\eta$ , получаемых, если положить  $\varphi = 0$  [т. е. при изменении числа  $\rho$  в ее разложении  $(a, b, c) = \rho(\xi_1 x + \xi_2 y) \times \times \frac{1}{\rho}(\eta_1 x + \eta_2 y)$ ], периодически совмещаться с собой. Каждая такая решетка  $\Gamma$  имеет свой вполне определенный конечный наименьший гиперболический угол совмещения с собой, так называемый ее *угол Пелля*  $\Pi$ . Если дана неопределенная тройничная квадратичная форма  $f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'x''x + 2b''xx'$ , коэффициенты которой пропорциональны целым числам, то, если положить  $f(x, x', x'') = 0$ , получится некоторый конус  $K$  второго порядка, и если рассматривать целочисленные линейные унимодулярные преобразования  $\Lambda$  пространства  $(x, x', x'')$ , при которых этот конус совмещается с собой (преобразования Лорентца, соответствующие этой форме), и называть эквивалентными точки, переходящие одна

в другую при таких преобразованиях  $\Lambda$ , то можно внутри  $K$  тоже выделить фундаментальную область  $V$  такую, что: 1) каждая точка внутри  $K$  эквивалентна точке из  $V$ , 2) две различные точки внутри  $V$  неэквивалентны. Эта область  $V$  играет для целочисленной неопределенной тройничной формы  $f$  ровно ту же роль, какую играет угол Пелля  $\Pi$  для неопределенной двойничной целочисленной формы  $(a, b, c)$ .

Если для данной формы  $f$  найдена эта область, то можно решить задачу эквивалентности.

В работе Б. А. Венкова «Об арифметической группе автоморфизмов неопределенной квадратичной формы» \* устанавливается существование фундаментальной области  $V$  (удовлетворяющей условиям 1 и 2) для неопределенных целочисленных форм с  $n$  переменными сигнатуры  $n - 2$ , состоящей из конечного числа выпуклых пирамид с конечным числом граней.

### 13. Четвертая часть пятого раздела «Арифметических исследований», содержащая приложение теории тройничных квадратичных форм и исследования о числе классов

Эта часть, озаглавленная «Некоторые приложения к теории двойничных форм», изложена в пп. 286—307.

1. *Доказательство теоремы о родах:*  $\gamma = 2^{\lambda-1}$ . В п. 286 Гаусс, используя построенную им теорию тройничных форм, доказывает глубокую теорему: всякий класс главного рода получается удвоением (возведением в квадрат) некоторого класса. Делает он это так. Пусть  $F = (A, B, C)$  — некоторая двойничная квадратичная форма главного рода определителя  $D$ . Рассмотрим ей обратную форму  $F' = (A, -B, C)$  и будем представлять эту последнюю тройничной формой  $f = x^2 - 2yz$ . В силу вышеизложенной теории представления двойничных форм тройничной формой это возможно. Действительно,  $\Delta = 1$ , поэтому надо искать «значение»  $\sqrt{(A, B, C)} \pmod{D}$ , а в силу того, что форма  $F$  — главного рода (только тут учитывается то, что  $F$  — главного рода), можно показать, что такие «значения» имеются. Далее,

\* «Известия АН СССР», № 2, 1937.

в силу специальных свойств формы  $f$ , тройничная форма  $g$  определителя  $\Delta = 1$ , такая, что ее коэффициенты  $a, a', a'', b, b', b''$  удовлетворяют нужным условиям, тоже существует, причем для формы  $f$  и коэффициенты  $a'', b, b'$  формы  $g$  выходят целые, а полученная форма  $g$  определителя  $\Delta = 1$  оказывается неопределенной. Но так как выше было доказано, что имеется только один класс неопределенных тройничных квадратичных форм определителя  $\Delta = 1$  и что все они эквивалентны форме  $f$ , то форма  $g$  эквивалентна  $f$ . Можно, следовательно, найти хотя бы одно преобразование

$$\begin{array}{ccc} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{array}$$

формы  $f$  в форму  $g$ . Каждое из таких преобразований дает представление

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

формы  $F'$  формой  $f$ . Именно, мы будем иметь

$$A = \alpha^2 - 2\alpha'\alpha'', \quad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \quad C = \beta^2 - 2\beta'\beta''.$$

Если обозначить числа  $\alpha\beta' - \alpha'\beta$ ,  $\alpha'\beta'' - \alpha''\beta'$ ,  $\alpha''\beta - \alpha\beta''$  через  $a, b, c$ , то они будут взаимно простые, и мы будем иметь

$$D = b^2 - 2ac.$$

Но учитывая, как получается двойничная форма, которая есть композит двух двойничных квадратичных форм, можно непосредственным вычислением проверить, что форма

$$F = (A, B, C) = AX^2 + 2BXY + CY^2$$

при помощи подстановки

$$X = 2\beta'xx' + \beta xy' + \beta yx' + \beta''yy'; \quad Y = 2\alpha'xx' + \alpha xy' + \alpha yx' + \alpha''yy'$$

переходит в произведение

$$(2ax^2 - 2bxy + cy^2)(2ax'^2 - 2bx'y' + cy'^2),$$

т. е. в квадрат (в смысле композиции форм Гаусса) формы

$$(2a, -b, c),$$

а при помощи подстановки  $\beta', \beta, \beta^2, \beta''; \alpha', \alpha, \alpha, 2\alpha''$  — в квадрат формы

$$(a, -b, 2c).$$

Одна из этих двух форм, как легко видеть, собственно примитивная. Таким образом, всякая форма  $(A, B, C)$  главного рода есть квадрат некоторой собственно примитивной формы того же определителя.

Вернувшись к соображениям п. 261, мы видим, что раз всякий класс главного рода есть квадрат некоторого класса, то  $\delta = g$ . Теперь уже, сравнивая равенства  $h = g\gamma$  и  $h = \delta\alpha$ , мы видим, что число родов равно числу  $\alpha$  тех классов, квадраты которых суть главный класс. А это число, как показал Гаусс, равно  $\frac{1}{2}\chi = 2^{\lambda-1}$ . Число родов, значит, равно  $2^{\lambda-1}$ .

Гаусс говорит, что если он не ошибается, этот результат представляет собой, может быть, самое красивое, что удастся доказать о целочисленных двойничных квадратичных формах. С этим нельзя не согласиться, так как таким образом о таинственном числе классов  $h$  квадратичных форм с данным определителем (или, что все равно, числе классов идеальных делителей в данном квадратичном поле) получен глубокий и простой результат: если определитель  $D$  делится на разные простые числа и их число равно  $\lambda$  (иногда надо еще рассматривать модули 4 и 8), то число родов в точности равно  $2^{\lambda-1}$ , а, следовательно, число классов  $h$  есть кратное этого числа:  $h = g2^{\lambda-1}$ . Каково же число  $g$  классов в каждом роде — это неизвестно и до сих пор. Наиболее далекий в настоящее время полученный результат в этом вопросе состоит в том, что если  $D = b^2 - ac < 0$ , то, какое бы ни зафиксировать положительное число  $\varepsilon$ , для всех достаточно больших (по абсолютной величине)  $D$  имеют место неравенства

$$|D|^{\frac{1}{2}-\varepsilon} < h < |D|^{\frac{1}{2}+\varepsilon}$$

(результат Хейльбронна и Зигеля).

2. *Теория родов Гаусса с точки зрения теории алгебраических чисел.* После описания того, каким образом Гаусс доказал основную теорему о родах, стоит остановиться на том, что такое теория родов с точки зрения современной теории алгебраических чисел.

Дело в том, что определение понятия рода у Гаусса (см. стр. 916) очень формальное. К одному роду Гаусс относит те классы данного определителя, характер (Totalcharacter) которых одинаков. Можно подойти к понятию рода гораздо более по существу, если опираться на теорию алгебраических чисел.

Заметим прежде всего, что простые числа, которые представляют хотя бы одной из форм данного определителя, это те и только те простые числа, по которым число  $4D$  есть квадратичный вычет, а тогда, как это следует из закона взаимности, это те и только те простые числа, которые содержатся хотя бы в одной из конечного числа некоторых определенных прогрессий:  $4Dt + l_1$ ,  $4Dt + l_2$ ,  $\dots$ ,  $4Dt + l_k$  (см. стр. 902).

Известно, что аналогичное утверждение не имеет места для отдельного класса форм. Например, для формы  $x^2 + xy + 6y^2$  определителя 23 нельзя указать таких прогрессий:  $Nt + l_1$ ,  $Nt + l_2$ ,  $\dots$ ,  $Nt + l_k$ .

Возникает следующая задача: каким образом можно так разбить все  $h$  классов  $K_1, \dots, K_h$  квадратичных форм данного определителя на группы  $(K_1, \dots, K_{r_1})$   $(K_{r_1+1}, \dots, K_{r_2})$   $\dots$   $(\dots K_h)$ , такие, что для того, чтобы простое число  $p$  представлялось хотя бы одним из классов заданной группы, было бы необходимо и достаточно, чтобы оно содержалось хотя бы в одной из некоторых заданных прогрессий.

Разбиение, при котором все классы попадают в одну группу, этому условию удовлетворяет, а разбиение, при котором каждый класс образует отдельную группу, вообще говоря, не удовлетворяет. Интересно найти, конечно, разбиение на такие самые маленькие группы, которые этому условию удовлетворяют. Таким разбиением является разбиение на роды.

Для того чтобы доказать это обстоятельство, обратимся к теории алгебраических чисел.

Пусть  $K$  — произвольное нормальное поле алгебраических чисел, и оно получается от расширения поля  $R$  рациональных чисел присоединением к нему целого алгебраического числа  $\alpha$ , и  $p$  — какой-нибудь простой идеальный делитель поля  $K$ , не входящий в дискриминант числа  $\alpha$ , а  $p$  — то натуральное простое число, которое делится на  $p$ . Легко показать, что существует одна и только одна подстановка  $s$  группы Галуа  $\mathfrak{G}$  поля  $K$ , для которой выполняется сравнение

$$\alpha/s \equiv \alpha^p \pmod{p}.$$

В таком случае говорят, что простой делитель  $p$  принадлежит «в смысле Фробениуса» к автоморфизму  $s$  поля  $K$ . Другие простые делители числа  $p$  принадлежат, в этом смысле, к подстановкам, сопряженным с  $s$ , и поэтому говорят, что простое натуральное число  $p$  принадлежит «в смысле Фробениуса» к классу сопряженных подстановок группы  $\mathfrak{G}$ . Очевидно, что всякое натуральное простое число  $p$ , не входящее в дискриминант числа  $\alpha$ , принадлежит, в этом смысле, к одному и только одному классу сопряженных подстановок группы  $\mathfrak{G}$ . Поэтому все натуральные простые числа  $p$ , кроме конечного их числа, разбиваются относительно поля  $K$  на классы Фробениуса, число которых равно числу классов сопряженных элементов группы  $\mathfrak{G}$ .

Н. Г. Чеботарев доказал важную теорему о том, что к любому классу сопряженных элементов группы  $\mathfrak{G}$  принадлежит, в указанном смысле, бесконечно много простых чисел  $p$ .

Можно показать, что если  $\bar{K}$ , тоже нормальное над  $R$ , подполе поля  $K$ , то всякий класс Фробениуса поля  $\bar{K}$  есть совокупность нескольких целых классов Фробениуса поля  $K$ .

Если поле  $K$  есть поле деления круга на  $m$  частей, то каждый класс сопряженных подстановок его группы  $\mathfrak{G}$  состоит только из одной подстановки (так как  $\mathfrak{G}$  абелева). Простые числа  $p$ , принадлежащие к данной подстановке поля деления круга, суть, как легко показать, не что иное, как все простые числа некоторой арифметической прогрессии  $mt + l$ , где  $l$  — то или иное из  $\varphi(m)$  чисел, меньших  $m$  и взаимно простых с  $m$ , в зависимости от того, какую из  $\varphi(m)$  подстановок мы рассматриваем.

Всякое абелево над  $R$  поле алгебраических чисел есть некоторое подполе некоторого поля деления круга (теорема Кронекера — Вебера), и поэтому, учитывая вышесказанное, получается, что класс Фробениуса для абелева поля есть совокупность всех простых чисел, представляемых некоторыми прогрессиями  $mt + l_1, mt + l_2, \dots, mt + l_r$ .

При помощи теории поля классов можно доказать следующую теорему.

Пусть  $R(\sqrt{d})$  — квадратичное поле определителя  $d$ . И пусть  $K$  — наибольшее абелево над  $R(\sqrt{d})$  неразветвленное его расширение, т. е. наибольшее поле алгебраических чисел, которое получается от присоединения к полю  $R(\sqrt{d})$  корня абелева, относительно него, уравнения с коэффициентами из этого поля, относительный дискриминант которого по отношению к полю  $R(\sqrt{d})$  равен 1. Как это доказывается в теории поля классов, группа Галуа  $G$  (абелева) этого поля  $K$  по отношению к полю  $R(\sqrt{d})$  изоморфна группе классов идеалов поля  $R(\sqrt{d})$  и имеет, следовательно, порядок  $h$ . Степень поля  $K$  над рациональным полем равна  $2h$ ; поле  $K$  относительно рационального поля тоже нормальное поле, но его группа Галуа  $\mathfrak{G}$  относительно рационального поля  $R$  уже, вообще говоря, не абелева.

Легко видеть, что если подстановка  $s$  группы  $\mathfrak{G}$  входит в ее подгруппу  $G$ , то класс сопряженных с  $s$  в группе  $\mathfrak{G}$  подстановок состоит из двух подстановок  $s$  и  $s^{-1}$ . При помощи теории поля классов можно показать, что те простые числа  $p$ , которые представляются данным примитивным классом квадратичных форм определителя  $d$  (без двоек при  $b$ ), суть те и только те простые числа, которые в поле  $K$  принадлежат «в смысле Фробениуса» к классу  $s, s^{-1}$  сопряженных подстановок группы  $\mathfrak{G}$ , образуемых той подстановкой  $s$  группы  $G$ , которой соответствует рассматриваемый класс квадратичных форм.

Из этой теоремы получается два следствия.

I. Все простые числа  $p$ , представляемые формами, принадлежащими к разным, но не обратным друг другу классам примитивных форм данного определителя  $d$ , различны, а представляемые формами

обратных классов — одинаковы. Последнее — очевидно, так как форме  $(a, b, c)$  обратна форма  $(a, -b, c)$ , а эти формы, очевидно, представляют одинаковые числа при  $x = m, y = n$  и  $x = m, y = -n$ .

II. Всякая примитивная форма представляет бесконечно много простых чисел, — это следует из теоремы Чеботарева для рассматриваемого поля  $K$ , но может быть, правда, доказано и минуя теорему Чеботарева.

Перейдем теперь к разбиению классов  $K_1, \dots, K_h$  на группы  $(K_1, \dots, K_{r_1}), (K_{r_1+1}, \dots, K_{r_2}), \dots (\dots K_h)$ , о которых мы говорили выше.

Рассмотрим наибольшее абелево над  $R$  подполе  $\bar{K}$  поля  $K$ , рассматривавшегося нами сейчас. Само поле  $K$  (степени  $2h$ ) тоже может быть абелевым над  $R$ , но может им и не быть. Во всяком случае, квадратичное его надполе  $R(\sqrt{d})$  абелево над  $R$ ; поэтому та подгруппа  $H$  группы  $\mathfrak{G}$  поля  $K$ , которой принадлежит  $\bar{K}$ , есть подгруппа группы  $G$ . При помощи теории поля классов можно показать, что ее подстановкам соответствуют классы главного рода, а подстановкам смежных с  $H$  в  $G$  систем — классы других родов.

Таким образом, теория родов связана с вопросом о наибольшем абелевом относительно  $R$  подполе, которое содержится в так называемом абсолютном поле классов  $K$  рассматриваемого квадратичного поля  $R(\sqrt{d})$ .

Если поле  $K$  само абелево, то  $H = 1$  и главный род, а следовательно, и все роды, имеют по одному классу. Другой крайний случай, когда наибольшее абелево подполе  $\bar{K}$  есть поле  $R(\sqrt{d})$ ; тогда  $H = G$  и все классы образуют один род. Но могут быть и промежуточные случаи.

Классы Фробениуса поля  $\bar{K}$  суть некоторые комплексы классов Фробениуса поля  $K$ , но какие?

Разложим группу  $\mathfrak{G}$  поля  $K$  на смежные системы по ее подгруппе  $H$ :

$$\mathfrak{G} = H + s_2 H + s_3 H + \dots + s_r H;$$

тогда эти смежные системы своей композицией образуют группу  $\mathfrak{G}$  поля  $\bar{K}$ . Так как группа  $\mathfrak{G}$  абелева, то классы ее сопряженных



элементов совпадают с отдельными ее элементами. Так как  $H \subset G$ , то у каждой из этих смежных систем либо все ее элементы лежат в  $G$ , либо все не лежат в  $G$ , в зависимости от того, лежит ли в  $G$  соответствующий коэффициент разложения  $s_i$ . Поэтому те из этих систем, которые лежат в  $G$ , суть просто все смежные системы  $G$  по  $H$ . Классы Фробениуса поля  $K$ , соответствующие классам  $s, s^{-1}$  сопряженных в  $\mathfrak{G}$  элементов, где  $s$  — подстановка  $G$ , как можно показать, объединяются в некоторые классы Фробениуса поля  $\bar{K}$ , если объединять те из них, у которых  $s$  принадлежит одной и той же смежной системе  $G$  по  $H$ . Отсюда, учитывая сказанное выше, и получается, что совокупность простых чисел  $p$ , представляемых хотя бы одной из форм одного и того же рода, есть не что иное, как некоторый класс Фробениуса поля  $\bar{K}$ . Но так как поле  $\bar{K}$  абелево, то эта совокупность простых чисел  $p$  есть не что иное, как совокупность всех простых чисел  $p$ , представляемых некоторыми определенными прогрессиями.

Итак, разбиение классов на роды есть одно из разбиений на группы, о которых мы говорили выше. Можно из этих же соображений показать, что не может быть более дробного такого разбиения.

Совершенно иной подход к теории родов квадратичных форм следующий.

Две целочисленные квадратичные формы  $f$  и  $g$  с  $n$  переменными и матрицами  $A$  и  $B$  называются *принадлежащими к одному и тому же роду*, если для любого целого  $q$  существует такая матрица с рациональными элементами  $T$ , что  $T^*AT = B$  и знаменатели всех элементов  $T$  взаимно просты с  $q$ .

Этот подход к теории родов ценен тем, что он сразу охватывает квадратичные формы с любым числом  $n$  переменных. К сожалению, мы не имеем возможности останавливаться на этой теории родов.

Можно показать, что две формы принадлежат к одному и тому же роду, если они целочисленно  $p$ -адически эквивалентны при любом  $p$  и, кроме того, вещественно эквивалентны.

3. *Дальнейшие приложения теории тройничных квадратичных форм.* Вернемся к дальнейшему описанию содержания четвертой части пятого раздела «Арифметических исследований». После изложения в первых двух пунктах (пп. 286 и 287) этой части доказатель-

ства теоремы о родах Гаусс в дальнейших его пунктах (пп. 288—300) разбирает ряд классических задач, которые решаются при помощи построенной им теории. Задачи эти следующие: теория разложения чисел или двойничных квадратичных форм на три квадрата (пп. 288—292); доказательство теоремы, высказанной Ферма, о том, что любое натуральное число может быть разложено на три треугольных числа или на четыре квадрата (как известно, эта последняя знаменитая теорема была впервые доказана Лагранжем) (п. 293). Что же касается теоремы, высказанной также Ферма, о том, что всякое натуральное число есть сумма пяти пятиугольных, шести шестиугольных чисел и т. д., то она была лишь гораздо позже доказана Коши. Далее Гаусс дает решение неопределенного уравнения  $ax^2 + by^2 + cz^2 = 0$  в целых числах (пп. 294—295), излагает соображения о методе, которым Лежандр пытался доказать закон взаимности (пп. 296—298); решает вопрос о представлении нуля любой тройничной квадратичной формой (п. 299); наконец, дает общее решение неопределенного уравнения 2-й степени с двумя неизвестными в рациональных числах (п. 300). В последних заключительных пунктах (пп. 301—307) Гаусс снова возвращается к двойничным квадратичным формам и рассматривает в п. 301 вопрос о среднем числе их родов, в пп. 302—304 — вопрос о среднем числе классов и, наконец, в пп. 305—307 — понятие о регулярных и иррегулярных определителях. Во всех этих пунктах Гаусс старается более глубоко, чем он это сделал до того, проникнуть в свойства группы классов квадратичных форм данного определителя, но исследования этих пунктов носят определенно незаконченный и фрагментарный характер.

Поясним, в чем они состоят.

4. *Исследования Гаусса о среднем числе классов.* Ввиду того, что число родов зависит от числа различных простых делителей определителя  $D$ , для ряда идущих подряд определителей  $\pm D$ ,  $\pm(D+1)$ ,  $\pm(D+2)$ , ... число родов скачкообразно, то увеличивается, то опять уменьшается; однако, как замечает Гаусс, если сложить число родов для идущих подряд определителей  $\pm D$ ,  $\pm(D+1)$ , ...,  $\pm(D+m-1)$  и разделить их на их число  $m$ , то получится «среднее» число родов, которое можно оценить. Для этого надо считать, что  $m$  берется очень большим (например, фик-

сированным), а затем  $D$  берется еще гораздо бóльшим, чем  $m$ . Гаусс говорит, что это среднее число родов может быть хорошо представлено формулой  $\alpha \log D + \beta$ , где  $\alpha$  и  $\beta$  — некоторые найденные им постоянные.

Аналогично Гаусс ставит вопрос о среднем числе классов данного определителя  $D$ , причем он получает, что «среднее» число классов может быть хорошо представлено формулой

$$\gamma \sqrt{D} - \delta,$$

где  $\gamma = \frac{2\pi}{7e}$ ,  $e = 1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} + \dots$ , а  $\delta = \frac{2}{\pi^2}$ . В связи с этим Гаусс получает следующую приближенную формулу

для числа  $\sum_{\Delta=1}^{\Delta \leq m} h(-\Delta)$  всех собственно примитивных классов всех отрицательных определителей, которые по абсолютной величине меньше или равны  $m$ :

$$\frac{2}{3} \gamma (\sqrt{m})^3 - \delta m,$$

где  $\gamma$  и  $\delta$  — числа, указанные выше.

Гаусс говорит, что он получил эту формулу «при помощи теоретических исследований» и что она очень близко сходится с тем, что он получил при помощи непосредственных численных проб. Сейчас можно только гадать, как Гаусс мог найти эту формулу, учитывающую и второй член  $-\delta m$ , в то время.

Формула эта была впервые доказана в работе 1918 г. И. М. Виноградовым со следующим остаточным членом:

$$\sum_{\Delta=1}^{\Delta \leq m} h(-\Delta) = \frac{4\pi}{24e} m^{\frac{3}{2}} - \frac{2}{\pi^2} m + O\left(m^{\frac{3}{4}} (\log m)^2\right).$$

5. *Дальнейшие исследования Гаусса о числе классов целочисленных двойничных квадратичных форм.* Среди посмертно (в 1876 г.) изданных работ Гаусса (Nachlass) имеются две статьи, озаглавленные «О связи между числом классов, на которые распадаются двойничные формы второй степени, и их определителем» (De nexu inter

multitudinem classium in quas formae binariae secundi gradus distribuuntur earumque determinantem) и доложенные Гёттингенскому королевскому обществу: первая — в 1834, а вторая — в 1837 г., но не напечатанные при жизни Гаусса.

Эти статьи заключают в себе дальнейшие исследования Гаусса о числе классов  $h$  целочисленных двойничных квадратичных форм данного определителя  $D$ . Обе эти статьи являются лишь незаконченными фрагментами. Однако из них видно, что Гаусс уже до Дирихле подошел к выводу тех же формул для числа классов, которые дал затем Дирихле в знаменитой своей работе 1840 г.: «*Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*»\*.

Вывод этих замечательных формул основан на двух различных способах найти некоторую «плотность». Первый способ дает эту плотность как произведение числа классов  $h$  на некоторую величину  $\kappa$ , которая легко вычисляется и выражается через дискриминант  $D$  и основное решение уравнения Пелля  $x^2 - Dy^2 = 1$ . Второй способ дает эту плотность в виде бесконечного ряда  $\sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n}$ , не зависящего (явно) от числа классов. Сравнение этих двух выражений этой плотности дает число классов  $h$ .

Из статей Гаусса ясно видно, что принципы для получения первого выражения искомой плотности у Гаусса и у Дирихле совпадают.

Что же касается второго выражения искомой плотности, то его Гаусс получил, по-видимому, уже очень давно (в декабре 1800 г.), но как он к нему пришел, из оставшихся после него фрагментов не вполне ясно. Путь, который, по-видимому, привел Гаусса к этому второму выражению, выясняет Дедекин в своих комментариях к этим работам Гаусса\*\*.

Поясним с той точки зрения, на которую мы стали на стр. 887, 892, о какой плотности идет речь и в чем состоит вывод первой формулы для нее. Пусть, например, задано вещественное квадратичное поле  $k$  и дискриминант его равен  $D$ , а число его классов  $h$ . Предположим для простоты (хотя и общий случай рассматривается совершенно аналогично), что не только решетка  $\mathcal{O}$

\* Dirichlet. Werke, Bd. I.

\*\* C. F. Gauss. Werke, Bd. II, стр. 292—303.

вещественная, но и все ее побочные решетки Клейна  $\mathcal{O}'$ ,  $\mathcal{O}''$ ,  $\dots$ ,  $\mathcal{O}^{(h-1)}$  тоже вещественные (дело в том, что даже при вещественности поля  $k$  некоторые из тех множителей  $\lambda_2, \lambda_3, \dots, \lambda_h$ , на которые мы помножали (стр. 892) представителей  $\mathfrak{F}_2, \mathfrak{F}_3, \dots, \mathfrak{F}_h$  идеалов неглавных классов, для того чтобы получилось правильное расположение решеток Клейна  $\mathcal{O}'$ ,  $\mathcal{O}''$ ,  $\dots$ ,  $\mathcal{O}^{(h-1)}$ , иногда могут получаться комплексными). Предположим также еще, что норма основной единицы  $\varepsilon_0$  положительная.

Рассмотрим *угол Пелля* кольца  $\mathcal{O}$ , т. е. угол, образованный произвольным лучом, исходящим из начала и лежащим в первом квадранте  $O\xi\eta$ , и тем лучом, в который он переходит при помощи того наименьшего «гиперболического» (относительно асимптот  $O\xi$ ,  $O\eta$ ) поворота плоскости, при котором решетка  $\mathcal{O}$  переходит в себя. Этот поворот получается от умножения всех точек плоскости на основную единицу  $\varepsilon_0$ .

Не только решетка  $\mathcal{O}$ , но и каждая отдельная из решеток  $\mathcal{O}'$ ,  $\mathcal{O}''$ ,  $\dots$ ,  $\mathcal{O}^{(h-1)}$ , периодична в том смысле, что она при этом гиперболическом повороте совмещается с собой. В силу этого совокупность всех точек системы  $\mathcal{O}^*$ , лежащих в таком углу Пелля, есть совокупность всех точек  $\mathcal{O}^*$  с положительной нормой, попарно не ассоциированных одна с другой, т. е. не отличающихся между собой лишь множителями единицы. Точки  $\mathcal{O}^*$ , лежащие во 2-м и 4-м квадрантах, имеют отрицательные нормы, а точки  $\mathcal{O}^*$ , лежащие в 3-м квадранте, ассоциированы с точками, лежащими в 1-м, при помощи единицы: — 1.

Обозначим через  $\Pi(t)$  ту часть угла Пелля, которая отрезается от него гиперболой  $\xi\eta = t$  (где  $t > 0$ ), и обозначим площадь  $\Pi(1)$  через  $\Pi_1$ ; в таком случае площадь области  $\Pi(t)$  равна  $t\Pi_1$ , так как область  $\Pi(t)$  получается из области  $\Pi(1)$  гомотетией с коэффициентом  $\sqrt{t}$  относительно начала координат.

Число  $T$  точек  $\mathcal{O}^*$ , лежащих в области  $\Pi(t)$ , представляет собой число всех различных идеалов поля  $k$  с положительными нормами, не превышающими  $t$ .

Ввиду того, что площади основных параллелограммов всех решеток  $\mathcal{O}$ ,  $\mathcal{O}'$ ,  $\mathcal{O}''$ ,  $\dots$ ,  $\mathcal{O}^{(h-1)}$  одинаковы и равны  $\sqrt{D}$ , что решетки эти попарно не имеют общих точек, кроме начала, и что число

точек решетки с данной площадью основного параллелограмма, принадлежащих данной области, приблизительно равно площади этой области, деленной на площадь этого параллелограмма, или, точно говоря (при увеличении коэффициента гомотетии  $\sqrt{t}$ ), асимптотически равно этому отношению, — число  $T$  точек  $\mathcal{O}^*$ , лежащих в  $\Pi(t)$ , асимптотически равно  $h \frac{t \Pi_1}{\sqrt{D}}$ . Отсюда следует, что предел

$$\lim \frac{T}{t} = h\kappa,$$

где  $\kappa = \frac{\Pi_1}{\sqrt{D}}$ . Этот предел называется *плотностью* идеалов поля  $k$ .

Это, попросту говоря, плотность точек системы  $\mathcal{O}^*$ , если за единицу площади принимать площадь  $\Pi_1$ .

Вывод второй формулы для этой «плотности» проводится так.

Пусть  $F(m)$  есть число различных идеалов поля  $k$  с положительной нормой  $m$ , т. е. число точек  $\mathcal{O}^*$ , лежащих на гиперболе  $\xi\eta = m$  в угле Пелля. Искомый предел

$$\lim \frac{T}{t} = \lim \frac{F(1) + F(2) + \dots + F(t)}{t}.$$

Но если расположить идеалы  $k$  с положительными нормами по увеличению нормы и они суть  $\mathfrak{F}_1, \mathfrak{F}_2, \dots, \mathfrak{F}_{T'}, \dots$ , а их нормы  $n_1 \leq n_2 \leq \dots \leq n_{T'} \leq \dots$ , то мы имеем очевидные неравенства  $F(1) + F(2) + \dots + F(n_{T'} - 1) < T' \leq F(1) + F(2) + \dots + F(n_{T'})$ , или, если разделить на  $n_{T'}$ , то неравенства

$$\begin{aligned} \frac{F(1) + F(2) + \dots + F(n_{T'} - 1)}{n_{T'} - 1} \left(1 - \frac{1}{n_{T'}}\right) &< \frac{T'}{n_{T'}} \leq \\ &\leq \frac{F(1) + F(2) + \dots + F(n_{T'})}{n_{T'}}, \end{aligned}$$

и поэтому, так как  $\lim_{T' \rightarrow \infty} \left(1 - \frac{1}{n_{T'}}\right) = 1$ , то, какое бы малое положительное  $\delta$  ни взять, мы будем, для всех достаточно больших  $T'$ , иметь  $h\kappa - \delta < \frac{T'}{n_{T'}} < h\kappa + \delta$ , или, деля на  $T'$ ,  $\frac{h\kappa - \delta}{T'} < \frac{1}{n_{T'}} < \frac{h\kappa + \delta}{T'}$ . Возведя все части этого последнего неравенства в  $s$ -ю

степень, где  $s > 1$ , умножая на  $(s - 1)$  и суммируя по всем  $T'$ , бóльшим некоторого достаточно большого  $T'_0$ , мы получим неравенства

$$(h\kappa - \delta)^s (s - 1) \sum_{T'} \frac{1}{T'^s} < (s - 1) \sum_{T'} \frac{1}{n_{T'}^s} < (h\kappa + \delta)^s (s - 1) \sum_{T'} \frac{1}{T'^s}.$$

Но известно: 1) что ряд  $\sum_t \frac{1}{t^s}$  при  $s > 1$  сходится и 2) что

$$\lim_{s \rightarrow 1} (s - 1) \sum_t \frac{1}{t^s} = 1.$$

Поэтому, приближая в предыдущих неравенствах  $s$  к 1, мы получим равенство

$$\lim \left( (s - 1) \sum \frac{1}{n(\mathfrak{F})^s} \right) = h\kappa. \quad (*)$$

Левая часть этого равенства является второй формулой для искомой «плотности»; она явно не зависит от  $h$ , в ней суммирование производится по всем идеалам поля  $k$  с положительной нормой.

Дальнейшее преобразование левой части этого равенства производится, во-первых, опираясь (два раза) на знаменитое «тождество Эйлера»  $\sum \frac{1}{n^s} = \prod \frac{1}{1 - p^{-s}}$ , где  $n$  пробегает все натуральные, а  $p$  — все простые числа, и которое имеет следующее обобщение на все идеалы  $\mathfrak{F}$  и все простые идеалы  $\mathfrak{p}$  некоторого поля  $k$ :

$$\sum \frac{1}{n(\mathfrak{F})^s} = \prod \frac{1}{1 - n(\mathfrak{p})^{-s}};$$

здесь  $n$  — значок нормы. Ряд  $\sum \frac{1}{n(\mathfrak{F})^s}$  называется *дзета-функцией Дедекинда* данного поля  $k$  и обозначается  $\zeta(s)$ .

Во-вторых, в этом преобразовании левой части равенства (\*) учитывается закон разложения натуральных простых чисел  $p$  на простые идеалы квадратичного поля  $k$ . Используя этот закон, можно получить, что

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} \prod_p \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}},$$

где  $\left(\frac{d}{p}\right)$  — символ Лежандра. Отсюда величина  $\lim ((s-1)\zeta(s))$ , называемая *вычетом* дзета-функции, получается равной

$$\lim \left( \left( (s-1) \prod_p \frac{1}{1-p^{-s}} \right) \prod_p \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} \right),$$

или, если учесть, что

$$\lim \left( (s-1) \prod_p \frac{1}{1-p^{-s}} \right) = \lim \left( (s-1) \sum \frac{1}{n^s} \right) = 1,$$

то

$$\lim ((s-1)\zeta(s)) = \lim \prod_p \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}.$$

Воспользовавшись снова тождеством Эйлера, но уже в обратном направлении, мы получаем

$$\lim ((s-1)\zeta(s)) = \sum \left(\frac{d}{n}\right) \frac{1}{n},$$

или, окончательно, формулу

$$h_K = \sum \left(\frac{d}{n}\right) \frac{1}{n},$$

которую уже знал Гаусс.

При помощи дальнейшего упрощения этой формулы получаются следующие формулы Дирихле для числа классов  $h$  квадратичного поля, которые содержат уже лишь конечные суммы.

В случае  $k(\sqrt{m})$ ,  $m < 0$

$$h = -\frac{w}{2|D|} \sum \left(\frac{D}{n}\right) \frac{1}{n}, \quad (n = 1, 2, \dots, |D|),$$

а в случае  $k(\sqrt{m})$ ,  $m > 0$

$$h = \frac{1}{2 \ln 2} \ln \frac{\prod_b \left( e^{\frac{b i \pi}{D}} - e^{-\frac{b i \pi}{D}} \right)}{\prod_a \left( e^{\frac{a i \pi}{D}} - e^{-\frac{a i \pi}{D}} \right)},$$



где  $\Pi$  распространены на все квадратичные вычеты  $a$  и квадратичные невычеты  $b \pmod{D}$ .

В течение 90 лет после опубликования этих формул Дирихле математикам не удавалось избавиться от средств анализа при выводе этих конечных формул, выражающих искомое натуральное число  $h$ . Первый, кто сдвинул этот вопрос, был Б. А. Венков. В своей работе «*Über die Klassenzahl positiver binärer quadratischen Formen*» (Math. Zschr., 1931, 33) он вывел формулы Дирихле при  $m < 0$  для случая  $d \not\equiv 1 \pmod{8}$  из совсем другого принципа, а именно, применяя арифметику кватернионов, вовсе не прибегая к средствам анализа, и тем самым более глубоко вник в чисто арифметические свойства этого числа.

6. *Регулярные и иррегулярные определители Гаусса и история теории абелевых групп.* В п. 305 Гаусс называет определитель  $D$  *регулярным*, если в главном роде есть такой класс, что всякий класс главного рода есть степень этого класса, т. е. если группа классов главного рода циклическая. Если определитель  $D$  *нерегулярный*, то эта группа — некоторая нециклическая абелева группа.

В п. 306 Гаусс говорит: «Относительно наиболее удобного расположения системы классов, которые содержатся в главном роде в случае иррегулярного определителя, мы здесь, ради краткости, говорить не будем; заметим только, что так как одного основания (базиса, производящего элемента — *Б. Д.*) в этом случае недостаточно, то необходимо брать два или даже еще большее число классов, при умножении и композиции которых получаются уже все остальные. При этом получаются двойные и кратные индексы, польза которых состоит примерно в том же, в чем состоит и польза простых индексов при регулярных определителях. Однако подробнее мы рассмотрим этот вопрос при другом подходящем случае». Насколько, однако, известно, не сохранилось записей Гаусса также и в его «Рукописном наследии», в которых была бы дана теорема о базисе абелевой группы.

В предисловии к своей известной работе «О группах перестановочных элементов» (1879) Фробениус и Штикельбергер говорят: «Основания теории конечных групп перестановочных элементов (конечных абелевых групп — *Б. Д.*) были положены, с одной стороны, Эйлером и Гауссом, а с другой, — Лагранжем и Абелем, первыми в их

арифметических исследованиях по теории степенных вычетов, а вторыми — в их алгебраических работах, относящихся к решению уравнений. После этих, положивших начало, исследований Гаусс и Шеринг продолжили эту теорию. Гаусс (Werke, II, 266; Nachlass, 1876) дает разложение группы на примарные группы, порядки которых взаимно простые (в прямое произведение таких групп — *Б. Д.*), а Шеринг (Gött. Nachr., 1869, Schering. Werke, Bd. I) дает ее разложение в элементарные группы, порядок каждой из которых делится на порядок следующей». Таким образом, теорему о базисе абелевой группы на примере гауссовой композиции классов впервые нашел Шеринг в 1869 г. В 1870 г. Кронекер перенес ее на абелевы группы вообще.

В этом месте стоит отметить, что в упоминавшейся не раз выше теории поля классов арифметический подход Эйлера и Гаусса и алгебраический подход Лагранжа и Абеля для случая абелевых групп оказываются как бы соединены и являются там двойственными описаниями одних и тех же фактов.

7. *Значение собственной эквивалентности в теории композиции классов Гаусса.* Поясним в заключение этого параграфа, какое преимущество имеет для теории композиции классов различение, делаемое Гауссом между собственной и несобственной эквивалентностью форм. Если классом считать, по Гауссу, совокупность собственно эквивалентных между собой форм, то получается группа классов, рассмотренная в теории композиции, изложенной выше. Если же, как это делал Лагранж, относить в один класс как собственно, так и несобственно эквивалентные между собой формы, то теория композиции запутывается. Действительно, формы  $(a, b, c)$  и  $(a, -b, c)$  несобственно эквивалентны одна другой, вторая получается из первой подстановкой  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . В смысле билинейной композиции произведение этих форм дает, как легко убедиться, главную форму  $(1, 0, L)$ , т. е. классы, соответствующие этим формам, обратные. Каждый класс Лагранжа есть, следовательно, сумма двух взаимнообратных классов Гаусса. Пусть имеются два класса Лагранжа  $a + a^{-1}$ ,  $b + b^{-1}$ , где  $a$  и  $b$  — классы Гаусса. Рассмотрим произведения  $ab$ ,  $a^{-1}b$ ,  $ab^{-1}$ ,  $a^{-1}b^{-1}$ . Из них  $ab$  и  $a^{-1}b^{-1}$  принадлежат взаимнообратным классам, а  $a^{-1}b$  и  $ab^{-1}$  — двум другим взаимнообратным классам. Поэтому

произведения форм двух классов Лагранжа дают не формы одного определенного класса Лагранжа, а формы одного или другого из некоторых двух классов Лагранжа. Поэтому композиция форм не ведет к группе композиции классов (в смысле Лагранжа), а к некоей мультигруппе.

#### 14. Шестой раздел «Арифметических исследований».

##### Различные приложения теории чисел

Раздел этот озаглавлен: «Различные применения предыдущих исследований» (пп. 308—334).

Гаусс начинает его словами: «Во многих местах до этого мы уже касались того, насколько высшая арифметика богата истинами, находящими применение также и в других частях математики; мы считаем, однако, небесполезным — специально рассмотреть некоторые приложения, которые заслуживают более подробного изложения, не столько для того чтобы исчерпать этот предмет, которым легко могли бы быть заполнены многие тома, сколько для того, чтобы на нескольких примерах пролить на него более яркий свет».

Гаусс подробно рассматривает решение следующих задач.

В пп. 309—311 рассматривается разложение дроби в сумму более простых дробей, основанное на теореме: если знаменатель  $n$  дроби  $\frac{m}{n}$  равен произведению взаимно простых чисел  $a, b, c, d, \dots$ , то можно представить дробь в виде

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \dots$$

В пп. 312—318 подробно рассматривается теория обращения обыкновенных дробей в десятичные.

В пп. 319—322 решается сравнение  $x^2 \equiv A \pmod{m}$ . Гаусс говорит, что, конечно, можно решать это сравнение при помощи таблиц индексов, но что делать, если вычисления выходят за пределы этой таблицы; поэтому Гаусс дает другой удобный способ, который он подробно разбирает.

В пп. 323—326 предлагается близкий к предыдущему способ для решения неопределенного уравнения  $mx^2 + ny^2 = A$ .

В пп. 327—328 дается другой способ решения сравнения

$$x^2 \equiv A \pmod{m}$$

для случая, когда  $A < 0$ .

В пп. 329—334 рассматриваются два различных способа узнавать, простое ли заданное число. Один основан на теории квадратичных вычетов, а другой — на одном соображении, связанном с теорией квадратичных форм.

## 15. Седьмой раздел «Арифметических исследований».

### Теория деления круга Гаусса

Этот последний раздел, озаглавленный «Об уравнениях, от которых зависит деление круга», посвящен одной алгебраической теории, в которой играют существенную роль некоторые соображения теории чисел, а именно теории уравнения  $x^n = 1$ .

Уравнение это называется *уравнением деления круга* потому, что корни его суть точки комплексной плоскости, лежащие на окружности радиуса 1 с центром в начале и делящие эту окружность на  $n$  равных частей.

1. *Возникновение этой теории у Гаусса и основной его результат.* В рассматриваемом седьмом разделе Гаусс строит во всех деталях для этого частного уравнения теорию, совпадающую с теорией Галуа (1811—1832). Галуа построил свою общую теорию алгебраических уравнений около 1830 г., т. е. через 30 лет после выхода в свет книги Гаусса, причем эта теория была опубликована лишь через 15 лет после смерти Галуа, в 1846 г., Лиувиллем, а сделалась общим достоянием алгебраистов только в конце 50-х годов прошлого столетия, после появления в свет курса высшей алгебры Серре. Теория Галуа имеет как бы две стороны — алгебраическую и арифметическую. Если подготовкой алгебраической стороны теории Галуа были работы по теории алгебраических уравнений Лагранжа, то подготовкой ее арифметической стороны была теория деления круга Гаусса. Сам Галуа в своем основном мемуаре ссылается на теорию деления круга Гаусса, которая, очевидно, послужила для него как бы прообразом при построении его общей теории.

Исследование уравнения  $x^n = 1$  дало, кроме того, Гауссу возмож-

ность решить знаменитый вопрос о том, каково должно быть число сторон правильного многоугольника для того, чтобы его можно было построить циркулем и линейкой. Оказалось, что кроме правильных многоугольников, у которых число сторон равно  $2^k$ ,  $3 \cdot 2^k$ ,  $5 \cdot 2^k$  или  $15 \cdot 2^k$ , возможность построения которых была известна уже древним, можно построить циркулем и линейкой многие другие, например, правильный семнадцатиугольник.

Это поразительное открытие Гаусс сделал еще до того, как он начал писать «Арифметические исследования». В июне 1796 г. в «Литературной газете», издававшейся тогда в Иене, была помещена следующая заметка:

#### «Н о в ы е о т к р ы т и я

Всякому начинающему геометру известно, что можно геометрически (т. е. циркулем и линейкой — *Б. Д.*) строить разные правильные многоугольники, а именно треугольник, пятиугольник, пятнадцатиугольник и те, которые получаются из каждого из этих путем последовательного удвоения числа его сторон. Это было уже известно во времена Эвклида, и, как кажется, с тех пор было распространено убеждение, что область элементарной геометрии дальше не распространяется: по крайней мере, я не знаю удачной попытки распространить ее в эту сторону. Тем более кажется мне заслуживающим внимания открытие, что кроме этих правильных многоугольников может быть геометрически построено еще множество других, например семнадцатиугольник. Это открытие является собственно лишь следствием одной еще не совсем законченной большой теории. Как только она получит эту законченность, она будет предложена публике.

К. Ф. Гаусс из Брауншвейга,  
Студент-математик в Геттингене».

В рассматриваемом седьмом разделе Гаусс доказывает, что если число  $n$  сторон правильного многоугольника имеет вид  $n = p_1 p_2 \dots p_l \cdot 2^k$ , где  $p_i, p_j, \dots, p_l$  — различные простые числа вида  $p = 2^m + 1$ , то он может быть построен циркулем и линейкой. (Для того чтобы число  $2^m + 1$  было простым, показатель  $m$  не должен иметь нечетных простых делителей, так как если бы  $m = qm_1$ , где  $q$  нечетное, то число это можно было бы написать так:  $2^m + 1 = (2^{m_1})^q + 1^q$ , но число это делится на  $2^{m_1} + 1$  и, следовательно, непростое. Показатель  $m$  здесь, следовательно, может быть сам только степенью двойки,  $m = 2^\mu$ , т. е. простые числа  $p_i, p_j, \dots$  имеют следующий вид:  $p = 2^{2^\mu} + 1$ .)

В предпоследнем п. 365 Гаусс говорит, что он имеет верный способ доказать и обратное, а именно, что ни при каких других  $p$ , кроме указанных, правильный многоугольник построить циркулем и линейкой уже нельзя. Он говорит далее, что «хотя границы настоящего сочинения не позволяют привести здесь это доказательство, мы считаем все же своим долгом указать на это, чтобы никто не надеялся бы свести еще и другие деления, кроме делений, дающихся нашей теорией, например, деления на 7, 11, 13, 19, ... частей, к геометрическим построениям (т. е. к построениям циркулем и линейкой — *Б. Д.*) и не тратил бы бесполезно свое время».

Доказательство этой обратной теоремы сразу следует из общей теории Галуа, но оно может быть проведено и непосредственно.

Перейдем теперь к изложению содержания самого седьмого раздела. В п. 336 Гаусс сводит задачу к случаю, когда  $n$  — простое число. В последующем изложении поэтому число  $n$  уже везде предполагается простым. В п. 341 дается доказательство того, что многочлен

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + x + 1 = X, \text{ где } n \text{ простое, не}$$

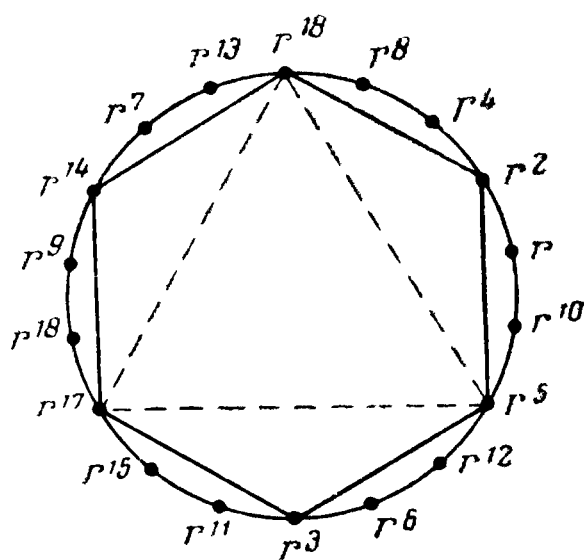
приводим в поле рациональных чисел. Доказательство это сложновато, сейчас найдены совершенно простые доказательства этого факта. Совокупность корней уравнения  $X = 0$  Гаусс обозначает через  $\Omega$ .

В п. 342 Гаусс кратко резюмирует, какую основную теорему он будет далее доказывать. Он говорит: *«Цель дальнейших исследований, указать которую представляется небесполезным, состоит в том, чтобы последовательно разлагать  $X$  на все большее и большее число сомножителей, причем так, чтобы их коэффициенты определялись при помощи уравнений по возможности более низких степеней, пока мы не дойдем таким путем до простых сомножителей, т. е. до самих корней из  $\Omega$ . Именно, мы покажем, что если число  $n - 1$  каким-либо способом разложено на целочисленные сомножители  $\alpha, \beta, \gamma, \dots$  (которые можно считать простыми числами), то  $X$  можно разложить на  $\alpha$  сомножителей степени  $(n - 1)/\alpha$ , коэффициенты которых определяются уравнением степени  $\alpha$ ; далее, что эти отдельные сомножители в свою очередь могут быть разложены на  $\beta$  сомножителей степени  $(n - 1)/\alpha\beta$  при помощи уравнения степени  $\beta$  и т. д., так что если  $\gamma$  обозначает число сомножителей  $\alpha, \beta, \gamma, \dots$ ,*

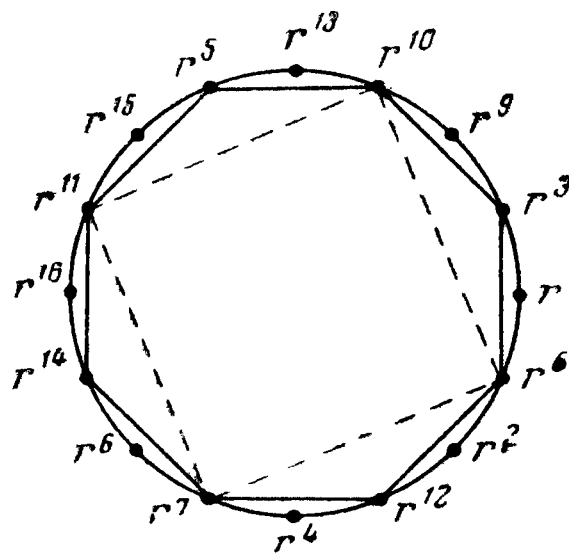
то нахождение корней из  $\Omega$  сводится к (последовательному — Б. Д. решению  $\gamma$  уравнений степеней  $\alpha, \beta, \gamma$  и т. д. Так, например, для  $n = 17$ , где  $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ , придется решить четыре квадратных, а для  $n = 73$  (где  $n - 1 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$  — Б. Д.) — три квадратных и два кубических уравнения».

2. Леммы о периодах и доказательство основной теоремы. Для доказательства этой основной теоремы Гаусс переходит к рассмотрению так называемых периодов.

Пункт 343 озаглавлен: «Все корни из  $\Omega$  разбиваются на некоторые классы (периоды)».



$$n=19, g_{19} = 2, (6, 2) \text{ и } (3, 16)$$



$$n=17, g_{17} = 3, (8, 3) \text{ и } (4, 10)$$

Дело в следующем. Пусть  $r$  — какой-нибудь из корней  $\Omega$ , тогда все корни  $\Omega$  суть  $r, r^2, r^3, \dots, r^{n-1}$ , что доказать нетрудно. Если теперь  $g$  — какой-либо первообразный корень простого числа  $n$ , то числа  $1, g, g^2, \dots, g^{n-2}$  представляют собой по модулю  $n$  числа  $1, 2, 3, \dots, n-1$ , но, может быть, взятые в другом порядке. Поэтому  $r, r^g, r^{g^2}, \dots, r^{g^{n-2}}$  — тоже все корни  $\Omega$ . Каждый из этих корней есть  $g$ -я степень предыдущего, а так как  $g^{n-1} \equiv 1 \pmod{n}$ , то  $(r^{g^{n-2}})^g = r^{g^{n-1}} = r$ , и поэтому первый из них есть в свою очередь  $g$ -я степень последнего.

Расположим мысленно эти корни последовательно, например, против часовой стрелки, в точках, делящих некоторую окружность на  $n-1$  равных частей (эта окружность не есть окружность комплексной плоскости) так, чтобы образовался правильный  $(n-1)$ -угольник  $P$ ; тогда  $g$ -я степень каждого из этих корней

будет равна последующему за ним. Пусть теперь  $n - 1 = ef$ . Посмотрим, какими свойствами обладают суммы по  $f$  этих корней такие, что соответствующие им  $f$  вершин многоугольника  $P$  образуют правильный  $f$ -угольник. Эти суммы Гаусс называет *периодами* длины  $f$ .

Если строить такую сумму, исходя от корня  $r^\lambda$ , то она будет равна

$$r^\lambda + r^{\lambda h} + r^{\lambda h^2} + \dots + r^{\lambda h^{f-1}}, \quad (\text{I})$$

где  $h = g^e$ , и каждое следующее ее слагаемое будет  $h$ -й степенью предыдущего и первое  $h$ -й степенью последнего. Гаусс обозначает эту сумму  $(f, \lambda)$ . Очевидно, что всё равно, с какой из его вершин начинать такой  $f$ -угольник, т. е. что  $(f, \lambda h^k) = (f, \lambda)$ . Если в формуле (I) положить  $\lambda = 0$  [или вообще  $\lambda \equiv 0 \pmod{n}$ ], то получится сумма  $(f, 0) = f$ ; эту сумму Гаусс тоже называет *периодом*. Но это особый период, не входящий в число тех, которые мы выше пояснили многоугольниками. Относительно периодов Гаусс доказывает ряд лемм.

**Лемма.** Произведение двух разных или одинаковых периодов одной и той же длины выражается линейно с целыми рациональными коэффициентами через периоды той же длины.

Например, если  $n = 19$ , т. е.  $n - 1 = 18$ , то

$$\begin{aligned} (6, 1)^2 &= (6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = \\ &= (6, 2) + 2(6, 8) + 2(6, 9) + 6. \end{aligned}$$

Эта лемма очевидна, так как при умножении  $(f, \lambda)$  на  $(f, \mu)$  надо составить сумму всех возможных произведений  $f$  корней, входящих в  $(f, \lambda)$  и  $f$  корней, входящих в  $(f, \mu)$  но эту сумму можно разбить на суммы тех  $f$  произведений, в которых расстояния по окружности против часовой стрелки корня из  $(f, \mu)$  от умноженного на  $(f, \mu)$  корня из  $(f, \lambda)$  одинаковы. Каждая из этих частных сумм произведений будет, очевидно, периодом той же длины  $f$ , или числом  $f$ , если показатели при  $r$  при этом получатся все делящиеся на  $n$ .

**Следствие.** Любая целая рациональная функция периодов одной и той же длины с рациональными коэффициентами равна линейной комбинации периодов этой длины с рациональными коэффициентами.



Это следствие получается повторным применением предыдущей леммы.

Лемма. Если  $\lambda$  не делится на  $n$ , то любой период  $(f, \mu)$ , где  $\mu$  тоже не делится на  $n$ , имеет следующее выражение через период  $(f, \lambda)$ , который мы обозначим тут через  $p$ , если  $n - 1 = ef$ :

$$\alpha + \beta p + \gamma p^2 + \dots + \vartheta p^{e-1}.$$

При доказательстве этой леммы Гауссу приходится использовать доказанную им в п. 341 неприводимость многочлена  $X$ .

Лемма. Всякий симметрический многочлен с рациональными коэффициентами от  $f$  корней периода длины  $f$  выражается линейно с рациональными коэффициентами через периоды длины  $f$ .

Эта лемма доказывается при помощи предыдущих лемм.

Лемма. Пусть  $n - 1 = \alpha\beta\gamma$  и пусть период  $(\beta\gamma, \lambda)$  состоит из  $\beta$  более коротких периодов  $(\gamma, \lambda), (\gamma, \lambda'), \dots$ ; тогда всякий симметрический многочлен с рациональными коэффициентами от этих более коротких периодов  $(\gamma, \lambda), (\gamma, \lambda'), \dots$  выражается линейно с рациональными коэффициентами через периоды длины  $\beta\gamma$ .

Эта лемма выводится из предыдущей леммы.

Применив эту лемму к частному случаю, когда рассматриваются элементарные симметрические функции от периодов  $(\gamma, \lambda), (\gamma, \lambda'), \dots$ , Гаусс получает, что то уравнение степени  $\beta$ , корнями которого являются эти периоды, имеет коэффициенты, выражающиеся линейно с рациональными коэффициентами через периоды длины  $\beta\gamma$ , откуда сейчас же и получается указанная выше основная его теорема.

Рассмотрим *пример*. Пусть  $n = 19$ , тогда  $n - 1 = 18 = 3 \cdot 3 \cdot 2$  и получается следующее разложение на периоды:

$$(18, 1) = \left\{ \begin{array}{ll} (6, 1) \left\{ \begin{array}{l} (2, 1) \dots r, r^{18} \\ (2, 8) \dots r^8, r^{11} \\ (2, 7) \dots r^7, r^{12} \end{array} \right. & \begin{array}{l} (6, 1), (6, 2), (6, 4) \text{ — корни} \\ x^3 + x^2 - 6x - 7 = 0; \end{array} \\ \\ (6, 2) \left\{ \begin{array}{l} (2, 2) \dots r^2, r^{17} \\ (2, 16) \dots r^3, r^{16} \\ (2, 14) \dots r^5, r^{14} \end{array} \right. & \begin{array}{l} (2, 1), (2, 8), (2, 7) \text{ — корни} \\ x^3 - (6, 1)x^2 + [(6, 1) + (6, 4)]x - \\ - 2 - (6, 2) = 0; \end{array} \\ \\ (6, 4) \left\{ \begin{array}{l} (2, 4) \dots r^4, r^{15} \\ (2, 1) \dots r^6, r^{13} \\ (2, 9) \dots r^9, r^{10} \end{array} \right. & \begin{array}{l} r, r^{18} \text{ — корни} \\ x^2 - (2, 1)x + 1 = 0. \end{array} \end{array} \right.$$

Если  $n = 2^m + 1$ , т. е.  $n - 1 = 2^m$ , то каждый из более длинных периодов раскладывается в сумму двух более коротких периодов и все уравнения цепи получаются квадратные, т. е. задача решения уравнения  $x^n - 1 = 0$  сводится к решению цепи квадратных уравнений.

Например, если  $n = 17$ , то  $n - 1 = 16 = 2 \cdot 2 \cdot 2 \cdot 2$  и получается такое разложение на периоды:

$$(16, 1) = \left\{ \begin{array}{l} (8, 1) \left\{ \begin{array}{l} (4, 1) \left\{ \begin{array}{l} (2, 1) \dots r, r^{16} \\ (2, 13) \dots r^4, r^{13} \end{array} \right. \begin{array}{l} (8, 1), (8, 3) \text{ — корни} \\ x^2 + x - 4 = 0; \end{array} \\ (4, 9) \left\{ \begin{array}{l} (2, 9) \dots r^8, r^9 \\ (2, 15) \dots r^2, r^{15} \end{array} \right. \begin{array}{l} (4, 1), (4, 9) \text{ — корни} \\ x^2 - (8, 1)x - 1 = 0; \end{array} \end{array} \right. \\ (8, 3) \left\{ \begin{array}{l} (4, 3) \left\{ \begin{array}{l} (2, 3) \dots r^3, r^{14} \\ (2, 5) \dots r^5, r^{12} \end{array} \right. \begin{array}{l} (2, 1), (2, 13) \text{ — корни} \\ x^2 - (4, 1)x + (4, 3) = 0; \end{array} \\ (4, 10) \left\{ \begin{array}{l} (2, 10) \dots r^7, r^{10} \\ (2, 11) \dots r^6, r^{11} \end{array} \right. \begin{array}{l} r, r^{16} \text{ — корни} \\ x^2 - (2, 1)x + 1 = 0. \end{array} \end{array} \right. \end{array} \right.$$

3. *Связь теории деления круга Гаусса с теорией Галуа.* Стоит отметить в этом месте, какую связь имеет эта основная теорема теории деления круга Гаусса с основной теоремой общей теории Галуа, доказанной Галуа через 30 лет после появления «Арифметических исследований» Гаусса.

Напомним, что Галуа начинает свою теорию с того, что если дано алгебраическое уравнение с коэффициентами, лежащими в некотором поле  $k$ , то можно свести его решение к решению некоторого другого, так называемого *соответствующего ему нормального*, уравнения с коэффициентами из того же поля  $k$ , т. е. такого: 1) которое неприводимо в поле  $k$ , и 2) все корни которого выражаются рационально через один из его корней и элементы поля  $k$ . Это замечание было сделано до Галуа еще Абелем.

Для нормального уравнения Галуа следующим образом вводит его группу. Если  $K$  — то поле, которое получается от расширения поля  $k$  присоединением к нему корня  $r$  заданного нормального уравнения  $m$ -й степени с коэффициентами из поля  $k$  и если  $\varphi_2(r)$ ,  $\varphi_3(r)$ , ...,  $\varphi_m(r)$  — другие его корни, то если во всех элементах поля  $K$  заменить  $r$  через  $\varphi_i(r)$ , то произойдет автоморфизм поля  $K$ ,

т. е. при такой замене элементы поля  $K$  перейдут в такие новые его элементы, что любое рациональное с коэффициентами из  $k$  соотношение между его элементами останется верным, если их заменить на те элементы, в которые они перешли. Эти  $m$  автоморфизмов поля  $K$  образуют группу — так называемую *группу Галуа*  $G$  над полем  $k$  рассматриваемого уравнения.

Основной результат теории Галуа состоит в следующем. Галуа вводит понятие нормального делителя группы. Если  $H$  — подгруппа  $G$ , то она называется *нормальным делителем*  $G$ , если для любого элемента  $g$  из  $G$  имеет место  $g^{-1}Hg = H$ , т. е. если  $H$  совпадает со всеми своими сопряженными.

Пусть  $F(x)$  — многочлен, стоящий в левой части рассматриваемого нормального уравнения, и пусть группа Галуа его имеет нормальный делитель индекса  $\alpha$  (т. е. такой, число элементов которого в  $\alpha$  раз меньше числа всех элементов группы); пусть этот нормальный делитель в свою очередь имеет нормальный делитель индекса  $\beta$  и т. д.; в таком случае, как это показывает Галуа (и это его основная теорема), многочлен  $F(x)$  разлагается на  $\alpha$  множителей степеней  $\frac{m}{\alpha}$ , коэффициенты которых выражаются рационально через корень уравнения степени  $\alpha$  с коэффициентами из поля  $k$ ; далее, каждый из этих множителей разлагается на  $\beta$  других множителей степеней  $\frac{m}{\alpha\beta}$ , коэффициенты которых выражаются рационально через корень уравнения степени  $\beta$ , коэффициенты которого выражаются рационально через корень предыдущего уравнения степени  $\alpha$  и элементы поля  $k$  и т. д. Но ведь это и есть теорема Гаусса, но для более общего случая.

Уравнение  $X = 0$  Гаусса степени  $m = n - 1$ , где  $n$  — простое число: 1) неприводимо в поле рациональных чисел и 2) все его корни выражаются рационально через один, т. е. оно нормально над полем  $k$  рациональных чисел. Корни его суть  $r, r^g, (r^g)^g, \dots$ , т. е. группа автоморфизмов — циклическая. Если порядок циклической группы равен  $m = \alpha\beta\gamma \dots$ , то оно имеет подгруппу индекса  $\alpha$ , которая тоже циклическая; эта подгруппа имеет в свою очередь подгруппу индекса  $\beta$ , которая тоже циклическая, и т. д. Но любая подгруппа циклической группы есть ее нормальный делитель. Таким

образом, мы видим, что основная теорема теории Галуа есть непосредственное обобщение теоремы Гаусса, о чем упоминает и сам Галуа.

Что же собственно понял Галуа? Галуа понял, что успех теории деления круга Гаусса основан совсем не на том, что уравнение  $X = 0$  имеет весьма специальный вид, а на том, что оно нормальное, и не на том, что его группа весьма специальная (циклическая), а на том, что все ее последовательные делители суть нормальные делители. Как только Галуа понял эти истинные причины успеха Гаусса — он построил свою общую теорию. Для этого, кроме того, ему должна была быть близка идея Лагранжа о том, что истинной «философией» теории алгебраических уравнений является теория подстановок.

4. *Вещественность всех корней всех промежуточных уравнений, кроме последнего, если оно квадратное.* В п. 355 Гаусс делает еще следующее замечание. Так как  $n$  нечетное, число  $n - 1$  четное. Множитель 2 числа  $n - 1$  можно, при разложении на периоды, всегда ставить на последнее место. Тогда разложение это кончится двучленными периодами  $(2, \lambda)$ . Если положить  $r^\lambda = \cos \frac{k 360^\circ}{n} + i \sin \frac{k 360^\circ}{n}$ , то  $r^{-\lambda} = \cos \frac{k 360^\circ}{n} - i \sin \frac{k 360^\circ}{n}$ . Но  $(2, \lambda) = r^\lambda + r^{\lambda h}$ , где  $h = g^e = g^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ , т. е.  $(2, \lambda) = r^\lambda + r^{-\lambda}$ . Поэтому  $(2, \lambda) = 2 \cos \frac{k 360^\circ}{n}$ . Двучленные периоды, таким образом, — вещественные числа, а следовательно, в выбранном разложении и все предыдущие им, более длинные, из них составленные периоды — тоже вещественные числа. При таком разложении на периоды, т. е. когда последние периоды, отличные от самих корней, двучленные, все вспомогательные уравнения, кроме последнего квадратного уравнения, дающего сами корни, имеют все корни вещественные.

Кроме того, получается, что  $\cos \frac{k 360^\circ}{n} = \frac{(2, \lambda)}{2}$ , где  $(2, \lambda)$  можно получить при помощи решения цепи уравнений с вещественными корнями.

Чтобы найти то  $\lambda$ , при котором  $k = 1$ , достаточно, очевидно, найти наибольший положительный двучленный период  $(2, \lambda)$ . Поступая таким образом в случае  $n = 17$ , т. е. решая вспомогательные

уравнения:  $x^2 + x - 4 = 0$ ;  $x^2 - (8, 1)x - 1 = 0$ ;  $x^2 - (4, 1)x + (4, 3) = 0$ , Гаусс находит, что

$$\cos \frac{360^\circ}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \\ + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Эта формула содержит только квадратные корни, которые могут быть, как известно, построены циркулем и линейкой. Она дает поэтому возможность дать построение циркулем и линейкой по радиусу окружности, который тут принят за 1, отрезка, равного  $\cos \frac{360^\circ}{17}$ , т. е. угла  $\frac{360^\circ}{17}$ , а следовательно, дает возможность построить циркулем и линейкой правильный семнадцатигульник.

5. *Разрешимость всех промежуточных уравнений в радикалах* Наконец, в п. 359 Гаусс показывает, что во всех случаях все вспомогательные уравнения решаются в радикалах. Он говорит:

«Предыдущие исследования относились к отысканию вспомогательных уравнений; *теперь мы изложим весьма выдающееся свойство, касающееся их решения*. Как известно, все усилия крупнейших математиков найти общее решение уравнений, степень которых выше четвертой, или (выражаясь точнее) найти **редукцию произвольных уравнений к чистым** (двучленным — *Б. Д.*) **уравнениям** до сих пор были тщетны, и едва ли можно сомневаться в том, что эта проблема не просто превосходит силы современного анализа, но и вообще неразрешима... Тем не менее очевидно, что существует бесчисленное множество смешанных (т. е. не двучленных — *Б. Д.*) уравнений любой степени, которые допускают такое сведение к чистым уравнениям, и мы надеемся, что математикам будет интересно, если *мы покажем, что наши вспомогательные уравнения всегда относятся к такому типу*». И далее Гаусс, используя резольвенты Лагранжа, доказывает, что все его вспомогательные уравнения решаются в радикалах.

Этим, по существу дела, и кончается знаменитое сочинение Гаусса «Арифметические исследования».

## 16. Гауссовы суммы

1. *Содержание работы Гаусса 1811 г.* В 1811 г. Гаусс опубликовал статью «Суммирование некоторых рядов особого вида» (*Summatio quarundam serierum singularium*). Гаусс начинает п. 1 работы следующей фразой: «Среди наиболее замечательных истин, к открытию которых проложила путь теория деления круга, далеко не последнее место занимает изложенное в п. 356 «Арифметических исследований» суммирование, причем не только вследствие его особенного изящества и исключительной плодотворности, более подробное обоснование которой мы отложим до другого исследования, но также и по той причине, что строгое и совершенное доказательство этого суммирования требует преодоления совсем необычных трудностей».

Дело идет о вычислении значений периодов длины  $m = \frac{n-1}{2}$ , где  $n$  простое, т. е. когда совокупность всех корней  $\Omega$  уравнения  $X = 0$  разбивается на два периода  $(m, 1)$  и  $(m, g)$ . В силу основной теоремы теории деления круга Гаусса не представляет труда составить то квадратное уравнение с рациональными коэффициентами, корнями которого являются эти периоды, но как узнать, какой из этих корней есть  $(m, 1)$ , а какой  $(m, g)$ , предполагая, что  $r = e^{\frac{2\pi i}{n}}$ ? Дело сводится к определению знака  $\pm$  в формуле для этих корней. И Гаусс говорит, что решение многих трудных вопросов теории чисел не отняло у него столько дней, сколько взяло лет работы решение вопроса об этом знаке. Выяснению этого вопроса посвящены пп. 5—32 работы; в п. 33 Гаусс показывает, что рассмотрение указанных периодов длины  $\frac{n-1}{2}$  дает также доказательство квадратичного закона взаимности.

Итак, периоды  $(m, 1)$  и  $(m, g)$  суть, в силу основной теоремы теории деления круга, корни некоторого квадратного уравнения

$$x^2 - Ax + B = 0$$

с рациональными коэффициентами.

Эти коэффициенты Гаусс в п. 356 «Арифметических исследований» находит так.  $A = (m, 1) + (m, g)$ , т. е. равно сумме всех корней уравнения  $X = x^{n-1} + x^{n-2} + \dots + x + 1 = 0$ , т. е. равно  $-1$ . Что же касается  $B$ , то оно равно  $(m, 1) \cdot (m, g)$ .

Это произведение в силу леммы, приведенной нами на стр. 961, может быть представлено в виде

$$(m, N + 1) + (m, N' + 1) + (m, N'' + 1) + \dots = W,$$

где слева  $m$  слагаемых, каждое из которых равно  $(m, 1)$ ,  $(m, g)$ , или  $(m, 0)$ . Таким образом,  $W = \alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$ , где  $\alpha, \beta, \gamma$  — целые положительные числа, причем  $\alpha + \beta + \gamma = m$ . Из доказательства леммы (стр. 961) сразу видно, что  $\beta = \gamma$  и что либо ни одно слагаемое  $W$  не равно  $(m, 0)$ , либо такое слагаемое только одно, т. е. что  $\alpha = 1$  или  $0$ . Таким образом, либо  $\alpha = 0, \beta = \gamma = \frac{1}{2}m$ , либо  $\alpha = 1, \beta = \gamma = \frac{1}{2}(m - 1)$ , а так как  $\alpha, \beta, \gamma$  целые, то первое имеет место, если  $m = \frac{n-1}{2}$  четное, т. е.  $n = 4l + 1$ , а второе, если  $m$  нечетное, т. е.  $n = 4l + 3$ . А так как  $(m, 0) = m = \frac{n-1}{2}$  и  $(m, 1) + (m, g) = -1$ , то в первом случае  $(m, 1) \cdot (m, g) = -\frac{1}{2}(n - 1)$ , а во втором  $\frac{1}{2}n$ ; поэтому искомое квадратное уравнение есть

$$x^2 + x - \frac{1}{4}(n - 1) = 0 \text{ или } x^2 + x + \frac{1}{4}(n + 1) = 0.$$

Периоды  $(m, 1)$  и  $(m, g)$  имеют следующий вид:

$$\begin{aligned} (m, 1) &= r + r^{g^2} + r^{g^4} + \dots + r^{g^{2(m-1)}}; \\ (m, g) &= r^g + r^{g^3} + r^{g^5} + \dots + r^{g^{2(m-1)+1}}, \end{aligned}$$

где  $r = e^{\frac{2\pi i}{n}}$ , т. е. они могут быть записаны и так:

$$(m, 1) = \sum_a e^{\frac{2\pi i}{n}a}, \quad (m, g) = \sum_b e^{\frac{2\pi i}{n}b},$$

где  $a$  пробегает все квадратичные вычеты, а  $b$  — все квадратичные невычеты по модулю  $n$ .

«Определение знака», таким образом, сводится к разысканию значения суммы:  $\sum e^{\frac{2\pi i}{n}a}$ . Оно проводится Гауссом в пп. 5 — 32

работы при помощи преобразования рассматриваемой суммы в произведение  $(r-r^{-1})(r^3-r^{-3})\dots(r^{p-2}-r^{-p+2})$ , что в свою очередь достигается при помощи исследования двух особых рядов:

$$f(x, m) = \sum_{j=1}^{\infty} (-1)^j (m, j) \quad \text{и} \quad F(x, m) = \sum_{j=1}^{\infty} x^{\frac{j}{2}} (m, j),$$

где  $(m, j) = \frac{(1-x^m)(1-x^{m-1})\dots(1-x^{m-j+1})}{(1-x)(1-x^2)\dots(1-x^j)}$ , каждый из которых

приводит Гаусса к желаемой цели.

Доказательство это принадлежит к числу трудных, поэтому мы его здесь воспроизводить не будем.

2. *Дальнейшие исследования о гауссовых суммах в XIX столетии.* В XIX в. рядом крупных математиков были предложены другие, отличающиеся от гауссова, решения вопроса о знаке в гауссовой сумме, основанные на разных принципах. В. А. Лебег (1840) прибег для этой цели к эллиптическим функциям; проще решил вопрос Коши (1840) и из тех же соображений в 1856 г. Кронекер. Дирихле (1837) определил значение гауссовой суммы при помощи определенного интеграла. Кронекер (1880) вернулся к способу, ранее предложенному Коши и основанному на основной теореме Коши о комплексном интегрировании.

Свойства гауссовых сумм были использованы при преобразовании ряда  $\sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n}$  в конечную сумму для вывода формул Дирихле числа классов  $h$  квадратичного поля.

Во всяком случае, можно сказать, что в течение ровно целого столетия после появления мемуара Гаусса 1811 г. совершенствовались решения вопроса, поставленного Гауссом, но никакого принципиального расширения задачи о гауссовых суммах получено не было. В статье Бахмана (P. B a c h m a n n. Über Gauss zahlen-theoretische Arbeiten), появившейся в 1911 г., гауссовым суммам посвящены только две страницы, причем Бахман, видимо, недоумевает, к чему относится замечание Гаусса о необыкновенной важности метода его сумм. Работы XIX в., посвященные теории гауссовых сумм, были замкнуты в узкие рамки.



3. *Второй этап развития теории тригонометрических сумм в аналитической теории чисел.* В 1914 г. были сделаны две совсем разные работы, с которых началось неожиданно мощное дальнейшее развитие метода тригонометрических сумм в теории чисел.

Две работы, о которых мы говорим, это работа Германа Вейля (H. Weyl) 1914 г., в которой была оценена абсолютная величина суммы:

$$\sum_{x=1}^p e^{2\pi i(\alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x)},$$

где  $\alpha_n, \alpha_{n-1}, \dots, \alpha_1$  — заданные действительные числа, причем хотя бы одно из них иррациональное, и работа И. М. Виноградова о распределении квадратичных вычетов. Хотя оценка Г. Вейля лишь немного лучше тривиальной  $\leq p$  (которая получается, если все слагаемые заменить 1), однако и она уж ведет к замечательным приложениям.

Используя ее, Харди и Литтлвуд создали первый мощный аналитический метод для решения аддитивных задач теории чисел. Осуществление этого метода Харди и Литтлвудом состоит в использовании целой цепи глубоких соображений, из которых главные: 1) применение интегрирования по контуру, 2) применение ряда Фарея, с которым связано разбиение контура интегрирования на большие и малые дуги (впервые примененное к подобным вопросам Вороным в его работе 1903 г.) и 3) использование неравенства Г. Вейля, которое позволяет оценивать интеграл по малым дугам.

Этим методом Харди и Литтлвуду удалось, в частности, дать более совершенное, чем у Гильберта, доказательство теоремы Варинга:  $N = x_1^n + x_2^n + \dots + x_k^n$ , — дающее асимптотическую формулу для числа представлений суммой  $k$   $n$ -х степеней целых чисел любого достаточно большого целого числа, из которой получилась хорошая оценка для числа  $k$  слагаемых, при которых уравнение Варинга имеет решение для любого такого  $N$ .

Метод Харди и Литтлвуда дал решение также ряда других важных задач.

Другая из двух упомянутых в начале этого пункта работ была работа И. М. Виноградова, которую он представил в 1914 г. на Математический факультет Петербургского университета для того, чтобы быть «оставленным при Университете для подготовки к про-

фессорскому званию» (напечатана она была позже, в 1918 г., в значительно расширенном виде). В этой работе, используя специальным образом гауссову сумму, Виноградов показывает, что абсолютная величина суммы символов Лежандра по  $p$ , подряд идущим натуральным числам, каково бы ни было  $p$ , не больше, чем  $\sqrt{p} \ln p$ , откуда, в частности, получается, что среди натуральных чисел, меньших  $\sqrt{p} \ln p$ , всегда есть хотя бы один квадратичный невычет модуля  $p$ .

Мы позволим себе привести это замечательное доказательство.

Но раньше сделаем несколько общеизвестных замечаний о гауссовых суммах. Во-первых, гауссова сумма  $\sum_r e^{\frac{2\pi i}{p} ar}$ , где  $r$  — все вычеты по модулю  $p$  и  $a$  не делится на  $p$ , легко сводится к сумме  $\sum_{x=0}^{p-1} e^{\frac{2\pi i}{p} ax^2}$ .

Действительно, слагаемое этой последней суммы при  $x=0$  равно 1, вычеты же  $(\bmod p)$  квадратов  $1^2, 2^2, \dots, (p-1)^2$  суть все квадратичные вычеты  $r(\bmod p)$ , но каждый взятый два раза, так как  $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2)$ , если  $x_1 + x_2$  делится на  $p$ , то  $x_1^2$  и  $x_2^2$  сравнимы  $(\bmod p)$ , если же нет, то не сравнимы. Вычеты  $(\bmod p)$  двух равно отстоящих от концов этого ряда квадратов поэтому одинаковы. Мы имеем, таким образом,  $\sum_{x=0}^{p-1} e^{\frac{2\pi i}{p} ax^2} = 1 + 2 \sum_r e^{\frac{2\pi i}{p} ar}$ .

Во-вторых, если  $n$  — все невычеты  $(\bmod p)$ , то

$$1 + \sum_r e^{\frac{2\pi i}{p} ar} + \sum_n e^{\frac{2\pi i}{p} an} = (m, 1) + (m, g) + 1 = 0;$$

поэтому

$$\sum_{x=0}^{p-1} e^{\frac{2\pi i}{p} ax^2} = \sum_r e^{\frac{2\pi i}{p} ar} - \sum_n e^{\frac{2\pi i}{p} an},$$

а так как  $\left(\frac{r}{p}\right) = +1$ ,  $\left(\frac{n}{p}\right) = -1$ , то

$$\sum_{x=0}^{p-1} e^{\frac{2\pi i}{p} ax^2} = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) e^{\frac{2\pi i}{p} am}.$$

Заметим еще, что модуль суммы  $\sum_{x=0}^{p-1} e^{\frac{2\pi i}{p} ax^2}$  равен  $\sqrt{p}$ . Это следу-

ет из того уравнения  $x^2 - Ax + B = 0$ , корнями которого являются периоды  $(m, 1)$  и  $(m, g)$ . Но сейчас это обычно выводят непосредственно так. Помножая сумму на её комплексно сопряженную

$\sum_{x=0}^{p-1} e^{-\frac{2\pi i}{p} ax^2}$ , получаем  $\sum_{x,y=0}^{p-1} e^{\frac{2\pi i}{p} a(x^2-y^2)}$ . Сделав здесь подстановку  $x=y+$

$+t$ , так как  $x^2 - y^2 = y^2 + 2ty + t^2 - y^2 = 2ty + t^2$ , получаем

$\sum_{t=0}^{p-1} e^{\frac{2\pi i}{p} at^2} \cdot \sum_{y=0}^{p-1} e^{\frac{2\pi i}{p} 2aty}$ . Но  $\sum_{y=0}^{p-1} e^{\frac{2\pi i}{p} 2aty}$ , если  $2at$  не делится на  $p$ , равно

нулю. Число  $2at$  делится на  $p$  только при  $t=0$ . Следовательно-

но, мы получаем  $e^{\frac{2\pi i}{p} a \cdot 0} \cdot \sum_{y=0}^{p-1} 1 = 1p = p$ . Таким образом, модуль ис-

следуемой суммы равен  $\sqrt{p}$ , а следовательно, сама эта сумма равна  $\varepsilon \sqrt{p}$ , где  $|\varepsilon| = 1$ .

Переходим теперь к доказательству теоремы Виноградова. Так

как  $\left(\frac{m}{p}\right) = \left(\frac{ma^2}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{ma}{p}\right)$ , то

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) e^{\frac{2\pi i}{p} am} = \left(\frac{a}{p}\right) \sum_{m=1}^{p-1} \left(\frac{ma}{p}\right) e^{\frac{2\pi i}{p} am} = \left(\frac{a}{p}\right) \sum_{m_1=1}^{p-1} \left(\frac{m_1}{p}\right) e^{\frac{2\pi i}{p} m_1} = \left(\frac{a}{p}\right) \varepsilon \sqrt{p},$$

откуда мы получаем

$$\left(\frac{a}{p}\right) = \frac{1}{\varepsilon \sqrt{p}} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) e^{\frac{2\pi i}{p} am}.$$

Просуммируем это равенство по  $a$  от 1 до  $p_1$ , где  $p_1$  — любое натуральное число:

$$\sum_{a=1}^{p_1} \left(\frac{a}{p}\right) = \frac{1}{\varepsilon \sqrt{p}} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \sum_{a=1}^{p_1} e^{\frac{2\pi i}{p} am}.$$

Перейдем к модулям (звездочками указаны ссылки на примечания):

$$\begin{aligned} \left| \sum_{a=1}^{p_1} \left( \frac{a}{p} \right) \right| &\leq \frac{1}{\sqrt{p}} \sum_{m=1}^{p-1} \left| \frac{e^{\frac{2\pi i}{p}(p_1+1)m} - e^{\frac{2\pi i}{p}m}}{e^{\frac{2\pi i}{p}m} - 1} \right| * \leq \\ &\leq \frac{1}{\sqrt{p}} \sum_{m=1}^{p-1} \left| \frac{2}{e^{\frac{\pi i}{p}m} (e^{\frac{\pi i}{p}m} - e^{-\frac{\pi i}{p}m})} \right| \leq \frac{1}{\sqrt{p}} \sum_{m=1}^{p-1} \frac{1}{\left| \sin \frac{\pi m}{p} \right|} ** = \\ &= \frac{2}{\sqrt{p}} \sum_{m=1}^{\frac{p-1}{2}} \frac{1}{\sin \frac{\pi m}{p}} ***. \end{aligned}$$

Но здесь  $0 < \frac{\pi m}{p} < \frac{\pi}{2}$ , а на интервале  $0 < x < \frac{\pi}{2}$ ,  $\frac{\sin x}{x} > \frac{\sin \frac{\pi}{2}}{\frac{\pi}{2}} = \frac{2}{\pi}$ ,

т. е.  $\sin x > \frac{2}{\pi} x$ . Другими словами,

$$\sin \frac{\pi m}{p} > \frac{2}{\pi} \cdot \frac{\pi m}{p} = \frac{2m}{p}.$$

Следовательно,

$$\left| \sum_{a=1}^{p_1} \left( \frac{a}{p} \right) \right| \leq \frac{2}{\sqrt{p}} \sum_{m=1}^{\frac{p-1}{2}} \frac{p}{2m} = \sqrt{p} \sum_{m=1}^{\frac{p-1}{2}} \frac{1}{m} < \sqrt{p} \ln p.$$

Этот метод был распространен И. М. Виноградовым на вопрос о распределении вычетов высших степеней и применен к ограничению наименьшего первообразного корня  $g$  простого числа  $p$ .

\* Если  $\sum_{a=1}^{p_1} e^{\frac{2\pi i}{p}am}$  рассмотреть как геометрическую прогрессию.

\*\* Здесь мы употребляем формулу Эйлера.

\*\*\* Здесь мы используем свойство, что равноотстоящие от концов суммы слагаемые равны.

Виноградов показал, что

$$g < 2^{2k} \sqrt{p} \ln p,$$

где  $k$  — число различных простых делителей.

Период, начавшийся в 1914 г. описанными выше работами Г. Вейля и И. М. Виноградова и по 1934 г., можно назвать вторым этапом развития теории тригонометрических сумм в теории чисел. По мнению И. М. Виноградова, характерными чертами этого этапа были две: 1) отказ от нахождения точных значений сумм и переход к их оценкам, но зато 2) освобождение от требования, чтобы высказывания, при их помощи получаемые, относились только к полной системе вычетов. Однако сохранялось условие, чтобы суммирование производилось по отрезку чисел натурального ряда, взятых подряд.

Уже в 1916 г. начали рассматривать куски полных рациональных тригонометрических сумм, причем трудности, возникающие при этом, не больше тех, какие имеются в теории иррациональных сумм (т. е. таких, как суммы Г. Вейля, где  $\alpha$ , иррациональные), так как многочлен с иррациональными коэффициентами все равно не периодичен по модулю  $p$ . Иногда даже и в случае рациональной суммы выгодно брать рациональные приближения коэффициентов, но зато с малыми знаменателями, как это делается в случае иррациональной суммы. В этот второй период были решены методом тригонометрических сумм многие важные задачи. Мы уже упоминали о знаменитых работах Харди и Литтльвуда. Были получены важные теоремы о распределении дробных долей многочлена, о представлении чисел в форме целого многочлена от многих переменных:

$$a_1 x_1^n + \dots + a_k x_k^n + \varphi(x_1, \dots, x_k)$$

(где  $\varphi$  — многочлен степени не выше  $n-1$ ), о некоторых системах диофантовых уравнений и т. д.

В 1928 г. Р. О. Кузьминым была получена следующая весьма общая оценка тригонометрической суммы. Если  $f(x)$  на отрезке  $a \leq x \leq b$  — такая функция, что  $\theta < f'(x) < 1 - \theta$  (где  $0 < \theta < \frac{1}{2}$ ) и

$$f'(x) \text{ монотонна, то } \left| \sum_a^b e^{2\pi i f(x)} \right| < \frac{2}{\theta}.$$

Здесь  $x$  пробегает все целые числа между  $a$  и  $b$  включительно. Геометрически это означает, что если имеется ломаная, состоящая из векторов длины 1, и такая, что каждый следующий вектор повернут относительно предыдущего на все больший и больший угол, заключающийся между  $\theta$  и  $1 - \theta$ , то конец этой ломаной лежит недалеко от ее начала.

Отметим, что в настоящее время знак гауссовой суммы, пожалуй, наиболее просто можно определить, используя эту лемму Кузь-

мина. А именно, полную гауссову сумму  $\sum_{x=1}^{p-1} e^{\frac{2\pi i}{p} x^2}$  нетрудно свести к вычислению двух следующих сумм:

$$W = \sum_{1 \leq x < \sqrt{p}} e^{\frac{2\pi i}{4p} x^2} \text{ и } Z = \sum_{\sqrt{p} < x \leq p-1} e^{\frac{2\pi i}{4p} x^2}.$$

Относительно  $W$  легко показать, что  $\operatorname{Re} \{(1 - i)W\} \geq \frac{1}{2} \sqrt{p}$ , где  $\operatorname{Re} \{ \}$  обозначает вещественную часть  $\{ \}$ . Что же касается до  $Z$ , то, применяя лемму Кузьмина, можно показать, что

$$|Z| \leq \sqrt{p}.$$

Соединяя оба эти обстоятельства, получаем определение знака в гауссовой сумме.

4. *Третий этап развития теории тригонометрических сумм в теории чисел.* Характерной чертой третьего этапа, начавшегося работой И. М. Виноградова 1934 г., является освобождение от того условия, чтобы суммирование проводилось по всем натуральным числам некоторого отрезка подряд. Так, чтобы было, например, возможно суммировать по простым числам или по числам, имеющим не более, чем столько-то простых множителей и т. д., И. М. Виноградов показал, что получаются хорошие оценки двойных сумм

$$\sum \sum e^{2\pi i f(x, y)}$$

по различным областям, где  $x$  и  $y$  пробегают достаточно густые независимые одна от другой последовательности целых чисел, и функция

$f(x, y)$  не разлагается в сумму двух функций, каждая от одной переменной. Этот способ оказался очень сильным; при помощи него И. М. Виноградов получил свою более тонкую оценку суммы Г. Вейля и оценки сумм, при помощи которых он доказал теорему Гольдбаха.

Конечно, мощный современный метод тригонометрических сумм, давший в последнее десятилетие столько глубоких теорем теории чисел, далеко ушел за рамки того, что дал Гаусс, но все же у истоков его стоит рассматриваемая работа Гаусса 1811 г. «Суммирование некоторых рядов особого вида».

5. *Причины успешного применения тригонометрических сумм в теории чисел.* Подобно тому, как это мы сделали в заключении параграфа об алгебраических числах, разумно и здесь поставить такой вопрос. Во-первых, говорит И. М. Виноградов, целые числа идут в ряду вещественных чисел периодически, и потому, очевидно, можно удобно описывать их свойства при помощи периодической функции  $e^{2\pi iz}$ . Но можно сделать и другое замечание. Тригонометрические суммы являются тем орудием, которое позволяет какую-нибудь искомую в теории чисел величину выразить формулой. Например, число решений сравнения

$$a_1x_1^n + a_2x_2^n + \dots + a_kx_k^n \equiv 0 \pmod{p},$$

где  $a_i$  — заданные целые числа, как нетрудно убедиться, равно

$$\frac{1}{p} \sum_{x_1=1}^p \dots \sum_{x_k=1}^p \sum_{a=1}^p e^{2\pi ia \frac{a_1x_1^n + \dots + a_kx_k^n}{p}}.$$

А когда искомое число записано формулой, то можно уже забыть задачу теории чисел и находить величину, определяемую формулой, или оценивать эту величину — это уже совсем другая задача, и часто, ввиду удобных свойств функции  $e^{2\pi iz}$ , ее можно решить.

Здесь мы видим аналогию тому положению, которое имеется в теории дифференциальных уравнений. Решая какую-нибудь задачу геометрии, механики или физики, составляют соответствующее ей дифференциальное уравнение; а затем занимаются второй, уже совсем другой задачей: как решить это уравнение; эта вторая задача основана на теоремах о дифференциальных уравнениях как таковых.

## СОДЕРЖАНИЕ

### АРИФМЕТИЧЕСКИЕ ИССЛЕДОВАНИЯ (*DISQUISITIONES ARITHMETICAE*)

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| Р а з д е л I. О сравнимости чисел вообще . . . . .                    | 15  |
| Р а з д е л II. О сравнениях первой степени . . . . .                  | 21  |
| Р а з д е л III. О степенных вычетах . . . . .                         | 50  |
| Р а з д е л IV. О сравнениях второй степени . . . . .                  | 94  |
| Р а з д е л V. О формах и неопределенных уравнениях второй степени     | 151 |
| Р а з д е л VI. Различные применения предыдущих исследований . . .     | 468 |
| Р а з д е л VII. Об уравнениях, от которых зависит деление круга . . . | 509 |
| Д о п о л н е н и я . . . . .                                          | 574 |
| Т а б л и ц ы . . . . .                                                | 576 |
| О г л а в л е н и е . . . . .                                          | 580 |

### ДРУГИЕ СОЧИНЕНИЯ

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| Новое доказательство одной арифметической теоремы . . . . .                                           | 587 |
| Суммирование некоторых рядов особого вида . . . . .                                                   | 594 |
| Новые доказательства и обобщения фундаментальной теоремы в учении<br>о квадратичных вычетах . . . . . | 636 |
| Теория биквадратичных вычетов. Сочинение первое . . . . .                                             | 655 |
| Теория биквадратичных вычетов. Сочинение второе . . . . .                                             | 686 |

### НЕКОТОРЫЕ ИССЛЕДОВАНИЯ ИЗ РУКОПИСНОГО НАСЛЕДИЯ ГАУССА

|                                                                                                |     |
|------------------------------------------------------------------------------------------------|-----|
| Учение о вычетах . . . . .                                                                     | 757 |
| I. Решение сравнения $X^m - 1 \equiv 0$ . . . . .                                              | 757 |
| II. Общие исследования о сравнениях . . . . .                                                  | 773 |
| Дальнейшее развитие исследований о чистых уравнениях . . . . .                                 | 807 |
| Доказательство некоторых теорем о периодах классов двойничных форм<br>второй степени . . . . . | 836 |



|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| О связи между числом классов, на которые распадаются двойничные формы второй степени, и их определителем . . . . . | 839 |
| Более подробное рассмотрение некоторых вопросов, относящихся к делению круга . . . . .                             | 867 |

ПРИЛОЖЕНИЯ

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| От редакции . . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 874 |
| И. М. Виноградов. Карл Фридрих Гаусс . . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 875 |
| Б. Н. Делоне. Работы Гаусса по теории чисел . . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 879 |
| 1. Теория чисел до Гаусса (879).— 2. «Арифметические исследования» Гаусса (880).— 3. О теории чисел вообще и о современных нам ее методах (882).— 4. О теории алгебраических чисел (885).— 5. Первый, второй и третий разделы «Арифметических исследований» Гаусса (895).— 6. Четвертый раздел «Арифметических исследований». Первое доказательство закона взаимности (897).— 7. Целые комплексные числа Гаусса и биквадратичный закон взаимности (900).— 8. О законах взаимности вообще и о задаче, которую они решают (902).— 9. О теореме Кронекера и о теории поля классов (904).— 10. Первая часть пятого раздела «Арифметических исследований» (906).— 11. Вторая часть пятого раздела «Арифметических исследований». Композиция классов и композиция родов квадратичных форм (914).— 12. Третья часть пятого раздела «Арифметических исследований». Отступление о тройничных формах (925).— 13. Четвертая часть пятого раздела «Арифметических исследований», содержащая приложение теории тройничных квадратичных форм и исследования о числе классов (939).— 14. Шестой раздел «Арифметических исследований». Различные приложения теории чисел (956).— 15. Седьмой раздел «Арифметических исследований». Теория деления круга Гаусса (957).— 16. Гауссовы суммы (967). |     |



*Карл Фридрих Гаусс*  
**Труды по теории чисел**

\*

*Утверждено к печати  
Редакционной коллегией серии «Классики науки»  
Академии наук СССР*

\*

Редактор издательства *А. З. Рывкин*  
Технический редактор *И. А. Макогонова*

РИСО № 2—103В. Сдано в набор 20/VI 1959 г.  
Подписано к печати 31/X 1959 г. Формат 70×92<sup>1</sup>/<sub>16</sub>  
Печ. л. 61,25. Усл. печ. л. 71,66. Уч.-изд. л. 49,8  
Изд. № 3675. Тип. зак. № 2078. Тираж 2500 экз.

*Цена 36 р. 85 к.*

Издательство Академии наук СССР  
Москва Б-62, Подсосенский пер., 21

---

2-я типография Издательства АН СССР  
Москва Г-99, Шубинский пер., 10